Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ЭЛЕКТРОННЫЕ ИНСТРУКЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 011

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ И. А. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЭЛЕКТРОННЫЕ ИНСТРУКЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Исполнитель:
обучающийся группы № ЗИБ –501 И. Е. Колотов
Руководитель:
кандидат педагогических наук,
доцент А. А. Шайдуров
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из сборника электронных инструкций для ООО «Нэт Бай Нэт Холдинг» и пояснительной записки на 63 страницах, содержащей 28 рисунков, 10 таблиц, 34 источников литературы, а также 1 приложение на 3 страницах.

Ключевые слова: Безопасность, инструкции, локальная сеть.

Колотов И. Е. Электронные инструкции по обеспечению безопасности локальной сети предприятия выпускная квалификационная работа / И. Е. Колотов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. —63 с.

В работе разработаны электронные инструкции для предприятия.

Цель выпускной квалификационной работы: разработать электронные инструкции по обеспечению безопасности локальной сети для ООО «Нэт Бай Нэт Холдинг».

Дано определение угроз и уязвимостей, рассмотрено их понятие и классификация. Выявлены основные системы и методы защиты от внутренних и внешних угроз. Проведена оценка состояния информационной безопасности в ООО «Нэт Бай Нэт Холдинг». Разработаны и внедрены электронные инструкции для организации ООО «Нэт Бай Нэт Холдинг».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Тема выпускной квалификационной работы является актуальной в наше время, так как безопасность локальной сети организации тесно связана с различными рисками, за счет внутренних и внешних угроз, которые могут привести к утечке конфиденциальной информации.

В зарубежных и отечественных публикациях часто делается акцент на то, что средства по злоупотреблению информацией, передаваемой в локальных сетях организаций, постоянно развиваются и совершенствуются и средства их предупреждения зачастую не всегда успевают за этой тенденцией. Поэтому для защиты информации в локальной сети мало использовать средство предупреждения, необходимо использовать комплекс мер защиты информации, который состоит из специальных средств, методов и мер, которые позволят предотвратить кражу информации.

Для обеспечения информационной безопасности информации в локальной сети предприятия необходимо в комплексе использовать различные методы. Организационные методы защиты информации заключаются в том, чтобы руководством были разработаны соответствующие инструкции, а также чтобы руководство своевременно принимала верные управленческие решения. Программные методы защита информации заключаются в том, чтобы применять специализированные программные средства, которые позволяют обеспечить защиту устройств с конфиденциальной информацией от атак и попыток несанкционированного доступа. Технические методы защиты информации заключается в том, чтобы использовать различные устройства, позволяющие обеспечить безопасность и защиту информации.

Большая часть решений, которые предлагаются современными компаниями, работающими на рынке информационной безопасности (ИБ), обеспечивают защиту информации в локальной сети от внешних угроз. Но суще-

ствуют еще и внутренние угрозы, при которых сотрудники компании являются потенциальными злоумышленниками.

Причем защититься от внутренних угроз намного сложнее, так как действия сотрудников сложнее предсказать, чем у внешних злоумышленников, особенно для тех сотрудников, у которых имеются возможности для несанкционированного доступа либо хищения информации. Если для сотрудников слишком грубо ограничить их возможности, это затруднит их работу, а в некоторых случаях сделает ее невозможной. Поэтому необходимо для каждого сотрудника, который имеет доступ к информации предприятия проводить консультации, давать методические указания, проводить тестирование полученных знаний в сфере безопасности.

Для того чтобы обеспечить защиту информации от внутренней и внешней угрозы нужно выбирать компромисс между организационными и техническими методами, при этом не нарушая потребность сотрудников и стремясь к максимальной защищенности.

Актуальность темы предопределила выбор направления исследования, цели и задачи работы.

Цель выпускной квалификационной работы: разработать электронные инструкции по защите локальной сети для общества с ограниченной ответственностью (ООО) «Нэт Бай Нэт Холдинг».

Для достижения поставленной цели в работе необходимо решить следующие задачи:

- дать определение угроз и уязвимостей, рассмотреть их понятие и классификацию;
- выявить основные средства и методы защиты от внутренних и внешних угроз;
- дать характеристику ООО «Нэт Бай Нэт Холдинг» и рассмотреть существующую организационную структуру компании;
- разработать и внедрить электронные инструкции по защите локальной сети предприятия ООО «Нэт Бай Нэт Холдинг».

Объект исследования — коммерческая организация ООО «Нэт Бай Нэт Холдинг».

Предмет исследования — информационная безопасность коммерческой организации.

Результатом выпускной квалификационной работы является разработка электронных инструкции по защите локальной сети предприятия.

Базовыми источниками при написании работы являются труды ученых в области информационной безопасности — С. К. Варлатой, Н. А. Гайдамакина, А. А. Змеева, С. Кораблева, С. Лихотинского, О. Лукоева, Н. А. Магомедовой, Т. И. Марковой, В. П. Мельникова, а также нормативные акты РФ — ФЗ № 98, ФЗ № 152, ФЗ № 184.

Для раскрытия поставленной цели и задач определена следующая структура исследования: работа состоит из введения, двух глав, заключения, списка использованной литературы. Названия глав отображают их содержание.

1 АНАЛИЗ ТЕОРЕТИЧЕСКИХ АСПЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

1.1 Понятие угроз и уязвимости информационной безопасности и их классификация

Рассматривая информационную безопасность необходимо дать определение таким понятиям как уязвимость и угроза, так как именно они и являются предпосылками информационной безопасности.

Понятие уязвимости в информационной безопасности произошло от английского слова «vulnerability», который в переводе означает недостатки в системе. Использование уязвимостей позволяет нарушителю намеренно похитить информацию, а так же нарушить целостность информационной системы или компьютерной сети. Уязвимость может появиться в случае ошибки программиста в коде при написании программы, из-за того что пользователь системы создал ненадежный пароль, который легко подобрать злоумышленнику, а так же благодаря вирусам и другим вредоносным программам, которые выявляются данные уязвимости и используют их в корыстных целях [1, с. 63].

Уязвимость информации – это возможность появления такой ситуации, при которой может быть реализована угроза безопасности информации, внешняя либо внутренняя. Причем борьба с внешними киберугрозами на сегодняшний момент реализуется лучше, с внутренними, так как по статистике 70% всех инцидентов безопасности связаны с внутренними угрозами.

Рассмотрим понятия внутренних и внешних угроз со стороны различных ученых в сфере информационной безопасности.

Так Д. Смирнов под внутренней угрозой понимает любые инциденты, при которых происходит утечка, блокирование либо искажение конфиденциальной информации, которая возникает в результате того, что сотрудники

компании преднамеренно либо в силу своей небрежности создали такую ситуацию. Исключением в данном случае является техногенная катастрофа, природные происшествия или форс-мажорные обстоятельства, ущерб от которых был получен по вине сотрудников компании [26].

Д. Р. Утебов рассматривая внутренние угрозы применительно к базам данных считает, что такую угрозу представляют люди, у которых имеется санкционированный доступ к базе данных [29, с. 29]. В данном случае подразумеваются специалисты компании, которые работают с информационными системами (пользователи), администрируют базы данных и информационные системы, а так же разработчики самописных приложений.

С. Кораблевым дается следующее определение внутренней угрозе: «Внутренняя угроза — это возможность несанкционированного доступа либо хищение данных сотрудниками предприятия» [8, с. 57].

О. Лукоев под внутренней угрозой информационной безопасности подразумевает случайную или преднамеренную утечку конфиденциальной информации, а так же нецелевое применение ресурсов предприятия [11, с. 101].

Под объектами внешней угрозы информационной безопасности (ИБ) будем понимать различные объекты информатизации — информационную систему, ее ресурсы, информационные технологии, программные средства и сети связи [19].

Рассматривая компьютерные сети предприятия под угрозой безопасности информации будем понимать такие действия либо события, при помощи которых изменяется функционирование компьютерной сети, при этом нарушается защищенность обрабатываемой в локальной сети информации [15, с. 97].

В качестве отличия внешних угроз от внутренних можно выделить тот факт, что при внутренней угрозе преступление совершает сотрудник компании доступными ему средствами, а при внешней угрозе нарушитель получает информацию посредством использования программно-аппаратных средств.

Как показывают исследования компании InfoWatch, специализирующейся на средствах защиты информации, в качестве одного из самых распространенных видов внутренней угрозы можно выделить утечку информации, так как пользователи информационной системы (инсайдеры) имеют легальный доступ к конфиденциальной информации, который нельзя закрыть в силу служебного положения. В связи с этим инсайдер может воспользоваться своим служебным положением и использовать конфиденциальную информацию в своих интересах [19].

Так как в крупных компаниях работает большое количество сотрудников, имеющих доступ к конфиденциальной информации различного характера, то потенциально возможных инсайдеров очень много.

Многими исследователями в сфере информационной безопасности выделяется большое количество разноплановых угроз безопасности информации различного происхождения, которые классифицируются по различным признакам [7, с. 102]

На рисунке 1 представлена одна из самых простых классификаций угроз информационной безопасности.

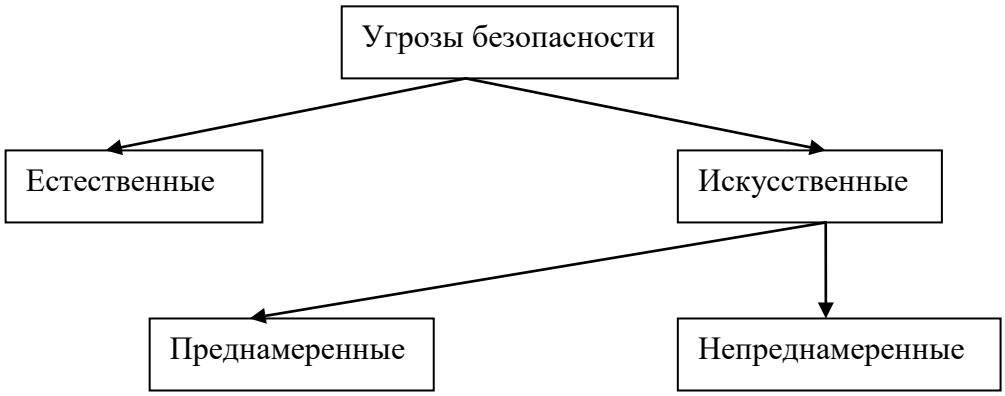


Рисунок 1 — Общая классификация угроз безопасности

Из рисунка 1 видно, что угрозы информационной безопасности подразделяются на естественные и искусственные, которые в свою очередь делятся на преднамеренные и непреднамеренные.

Естественные угрозы не зависят от воздействия человека и вызываются воздействием на технические каналы передачи информации и ее элементы,

объективными физическими процессами или стихийными природными явлениями.

Искусственные угрозы информационной безопасности вызваны воздействием человека на технические каналы передачи информации.

Непреднамеренная искусственная угроза является неумышленной или случайной и обычно появляется из-за ошибок в проектировании технических каналов передачи информации и ее элементов, а также ошибками, которые могут возникнуть в программном обеспечении.

Преднамеренная угроза информационной безопасности является наиболее встречающейся и самой опасной, так как связана с корыстными устремлениями злоумышленника.

Источники технических угроз по отношению к каналам передачи информации подразделяются на внешние и внутренние. Это могут быть компоненты компьютерной сети, различная аппаратура, информационные системы и программное обеспечение, а также персонал.

При анализе негативных последствий реализации технических угроз предполагается обязательная идентификация возможных источников угроз и уязвимостей, которые способствуют их проявлению и методам реализации. Модель реализации технических угроз информационной безопасности можно представить в виде схемы, представленной на рисунке 2.

Рисунок 2 — Модель реализации угроз информационной безопасности

Техническую угрозу можно классифицировать по возможности нанесения ущерба субъектам отношений при нарушениях целей безопасности. В случае обеспечения конфиденциальности информации угрозой может быть хищение или копирование информации, средств обработки информации, а также неумышленная потеря информации. В случае обеспечения целостности информации можно привести следующий список технических угроз: модификация или искажение информации, отрицание подлинности или навязывание ложной информации. В случае обеспечения доступности информации нарушитель может ее блокировать, а также уничтожить либо саму информацию, либо средства ее обработки.

Компания InfoWatch предлагает классификацию инсайдеров подразделяя их на 2 группы (лояльные и злонамеренные) и на 6 типов - халатный, манипулируемый, обиженный, нелояльный, подрабатывающий и внедренный.

В таблице 1 приведены сведения о целях, мотивации и последовательности действий каждого из перечисленных типов инсайдеров [13, с. 112].

Таблица 1 — Классификация инсайдеров

Тип	Корысть	Умысел	Действия при возможности	Постановка задачи
Халатный	Нет	Нет	Сообщение	Нет
Манипулируемый	Нет	Нет	Сообщение	Нет
Обиженный	Нет	Да	Отказ	Сам
Нелояльный	Нет	Да	Имитация	Сам
Подрабатывающий	Да	Да	Отказ, взлом, имитация	Извне, сам
Внедренный	Да	Да	Взлом	Извне

Халатные инсайдеры — это самый распространенный тип внутренних нарушителей, которые являются невнимательными и осуществляют нарушения случайно не имея такой цели, умысла или корысти. Этими сотрудниками создаются незлонамеренные ненаправленные угрозы, за счет нарушения правил хранения конфиденциальной информации, например, вынос информации из организации, для того чтобы поработать с ней дома или в командировке. В

результате конфиденциальная информация может быть утеряна или к ней появляется доступ посторонних личностей — членов семьи, знакомых и т.п.

Для предотвращения такого вида нарушений можно использовать простые технические средства предотвращения каналов утечек — контентная фильтрация исходящего трафика в сочетании с менеджерами устройств ввода — вывода.

Манипулируемый инсайдер, используя различные ухищрения, получает путем обмана персональную информацию пользователя (пароли, пинкоды, номера кредитных карт и т.п.).

Злонамеренные инсайдеры понимают, что выполняемые ими нарушения нанесут вред компании, в которой они работают и в зависимости от мотива враждебного действия, подразделяются на саботажников, нелояльных и мотивируемых извне.

Саботажник наносит вред предприятию исходя из личных мотивов, обид за недостаточную оценку его роли в компании, малую заработную плату и т.п.

Нелояльный инсайдер — это чаще всего сотрудник, который уже собирается увольняться и забирает с собой конфиденциальную информацию [13, с. 134].

Внутренние угрозы могут быть реализованы при разглашении конфиденциальной информации. Этот вид угроз подразумевает разглашение информации, которая представляет коммерческую тайну, при помощи отсылки данных посредством электронной почты, либо при помощи средств обмена мгновенными сообщениями, а также возможно с помощью копирования данных на переносной носитель либо просто распечатав эти данные на бумажный носитель.

Кража конфиденциальной информации может быть осуществлена при помощи неправомерного доступа к информации, особенно если информация передается по локальной сети обычным соединением без применения алгоритмов шифрования, а так же путем взлома корпоративной сети предприя-

тия. Так же возможно украсть информацию непосредственно с экрана монитора или с напечатанных материалов.

В случае нецелевого использовании ресурсов компании так же может возникнуть угроза информационной безопасности. Например, при посещении развлекательного сайта на компьютер может быть установлено потенциально опасное ПО, в случае скачивания и запуска неизвестных файлов. Кроме того, к данному виду угроз можно отнести использование ресурсов предприятия для рассылки различной информации рекламного характера, спама или информации личного характера, в том числе информации о сотрудниках, номерах социального страхования, кредитных карт и т.д. [32, с. 190].

Ассоциацией Computing Technology Industry Association четыре года проводилось крупное исследование возникающих на предприятиях внутренних угроз информационной безопасности и сопостовлялось с методами противодействия этим угрозам. Как показало исследование основной причиной нарушения является человеческая ошибка (60% нарушений информационной безопасности). При этом исследователи прогнозируют рост нарушений по вине человеческих ошибок. Для предотвращения или снижения рисков необходимо персоналу ИТ-подразделений, в обязанности которых входит обучение сотрудников правилам соблюдения информационной безопасности, обучать пользователей необходимым навыкам, с последующим тестирование полученных знаний.

Одни из самых распространенных каналов утечки информации — это нарушения, которые происходят при неумышленном раскрытии информации в следствие неосведомленности или недисциплинированности сотрудника. Умышленно информация распространяется намного реже, но в данном случае информация попадает целенаправленно и имеет более опасные последствия для организации.

В конфиденциальной информации наиболее заинтересованными являются конкуренты, в связи с этим инсайдеры представляют угрозу прежде всего для интеллектуальной собственности компании, которая является од-

ним из ее основных активов. В связи с этим необходимо на правовом уровне устанавливать и защищать права интеллектуальной собственности.

Угроза безопасности от внутренних угроз со стороны инсайдеров является реальной проблемой и одним из наиболее сложных вопросов, которые приходится решать иногда просто в силу должностей, занимаемых инсайдерами. По данным различных исследований, источники до 80% угроз информационной безопасности являются внутренними и находятся в самой организации [28].

При использовании компаниями современных информационных технологий тоже накладывают свои ограничения на информационную безопасность, так как благодаря смартфонам, ноутбукам и планшетам повышается мобильность сотрудников, тем самым расширяя сетевой периметр организации.

Действенность борьбы с инсайдерами сильно повышается в случае использования комплексных методов. Это может быть создание четкого классификатора данных по степени их критичности, эффективно работающая политики безопасность компании, внедренные программно-аппаратные средства контроля доступа, протоколирование событий пользователей и приложений, а также специальные средства мониторинга и управления обменом информации, функционирующие по ключевым словам.

Для того чтобы обеспечить необходимый уровень безопасности нужно минимизировать негативное влияние инсайдеров на бизнес предприятия при помощи своевременных средств их обнаружения, адекватного реагирования, предотвращения кражи конфиденциальной информации и применения к ним дисциплинарных и правовых мер пресечения.

Для решения этой непростой задачи нужно задействовать весь арсенал доступных средств, включая юридические, организационные и программно-технические механизмы защиты.

1.2 Системы и методы защиты корпоративной информации от внутренних и внешних угроз

Информационной безопасностью компании является комплекс действий и мероприятий, который исключает нанесение внутреннего ущерба коммерческой деятельности [10, с. 55].

Защитой информации является комплекс организационных, правовых и технических мер предназначенных для предотвращения угроз информационной безопасности и устранения их последствий [4, с. 72].

Организация защиты информации в компании является одним из самых важных моментов, который руководству компании ни за что нельзя упускать из вида, так как последствия могут быть очень серьезными в случае утраты базы данных, результатов аналитических исследований, исходных кодов или программных продуктов. В случае слабой организации защиты информации это может привести к достаточно проблематичному дальнейшему ведению бизнеса, а в определенных случаях может вообще сделать его невозможным.

Существующая на сегодняшний момент потребность руководства компаний в защите конфиденциальной информации, развитии IT-инфраструктуры и бизнеса в целом растет пропорционально росту угроз безопасности и киберпреступности. Большая часть крупных компаний уже ушла от точечных решений проблем информационной безопасности, выстраивая комплексную систему информационной безопасности, которая способна защищать их бизнес от различных уязвимостей и рисков.

В случае отсутствия системы информационной безопасности либо ее ненадлежащем качестве оставляет предприятие уязвимым перед внешними и внутренними воздействиями, повышая вероятность того, что конфиденциальная информация будет украдена. Обычные методы обеспечения информационной безопасности не смогут защитить предприятие от взлома компьютерной сети и кражи конфиденциальной информации.

Нужно стремиться к комплексной защите информации, которую можно подразделить на:

- защиту конфиденциальной информации, в которую входит коммерческая или служебная тайна;
- защиту персональных данных, в которую входят личные сведения сотрудников компании, клиенты и заемщики;
- информационную безопасность информационно-управляющих систем;
- защиту открытой информации, которая содержится в базах данных предприятия, в информационных системах документооборота, различных программных средствах компании [14, с. 68].

Информационная безопасность предприятия должна учитывать все события, в процессе которых информация может быть создана, изменена или удалена. Тогда система будет защищена, а также будет гарантирована точность и целостность имеющейся информации.

Руководителю предприятия необходимо осознавать исключительную важность внедрения инновационных решений и передовых продуктов, которые позволят обеспечить информационную безопасность компании. Для этого нужно заниматься проектированием, внедрением, интеграцией и обслуживанием решений в сфере безопасности и стремится к тому, чтобы портфель ИБ-решений постоянно качественно расширялся.

Комплексным подходом к проектам в области информационной безопасности предприятия можно выделить три основных этапа (рисунок 3):

- на первом этапе проводится анализ и оценка информационной безопасности предприятия для выявления наиболее уязвимых мест;
- на втором этапе внедряется система, при помощи которой будет обеспечиваться информационная безопасность;
- на третьем этапе производится поддержка полученных бизнес процессов для возможной корректировки в случае необходимости.

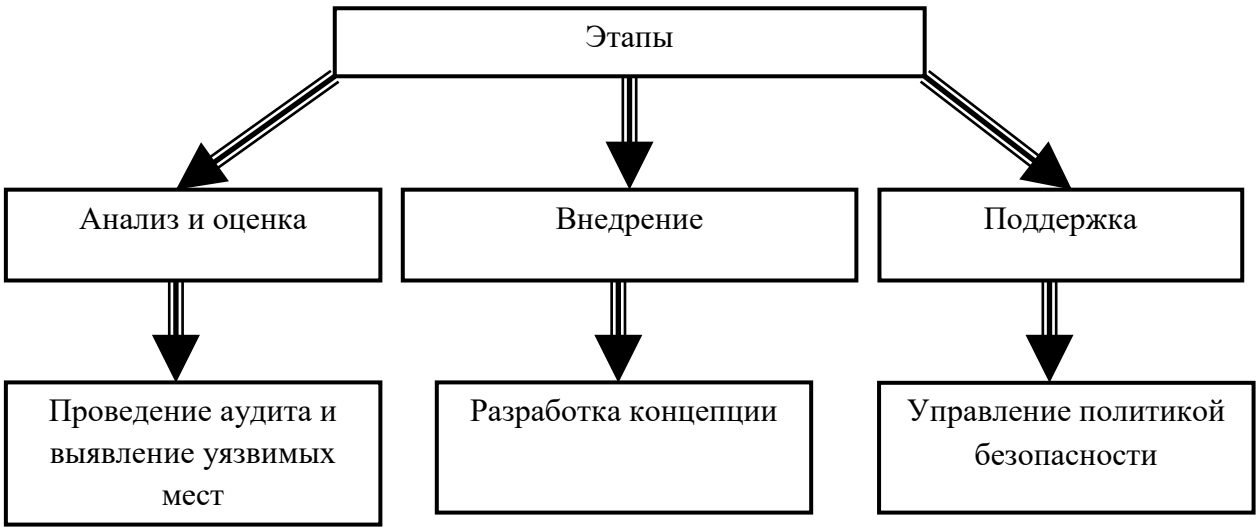


Рисунок 3 — Этапы информационной безопасности компании

В первый этап информационной безопасности входит выполнение следующих мероприятий:

- проведение аудита и выявление уязвимых мест информационной системы предприятия;
- разработка концепции информационной безопасности предприятия;
- внедрение и централизованное управление политикой безопасности и информационными рисками предприятия.

При проведении аудита информационной безопасности осуществляется независимая экспертиза проблемных областей функционирования предприятия для выявления уязвимостей. Проведение аудита информационных систем дает возможность:

- провести объективную качественной и количественную оценку информационной безопасности предприятия;
- рассмотреть реальное состояние защищенности ресурсов информационных систем, внедренных на предприятии;
- определить уровень возможностей, которые существуют в информационных системах предприятия, противопоставив их внешним и внутренним угрозам.

При проведении аудита информационной безопасности выполняются следующе функции:

1. Заинтересованная в аудите сторона (руководитель предприятия) решает провести аудит.
2. Проведение предварительного анализа, который состоит из:
   - определяются цели и задачи, для чего проводится аудит;
   - формулируются требования к информационной безопасности;
   - разрабатывается и согласовывается план и методика проведения аудита.
3. Собирается необходимая информация от аудита, в который входит:
   - получение необходимой документации от руководителя предприятия;
   - опрос IT-специалистов на предмет безопасности и работоспособности систем;
   - исследование структуры существующих информационных систем.
4. Анализируются данные полученные в результате аудита, проводимые при помощи следующих методов:
   - анализ рисков;
   - использование стандартов информационной безопасности предприятия;
   - комбинация первых двух параметров.
5. Оценивается информационная безопасность, в которую входит:
   - оценка рисков;
   - исследование имеющихся уязвимостей информационных системах предприятия;
   - анализируются угрозы информационной безопасности предприятия.
6. Обрабатываются результаты оценки.

7. Вырабатываются рекомендации по повышению уровня информационной безопасности предприятия [14, с. 47].

В результате проведения аудита информационной безопасности у руководителя предприятия появляются следующие преимущества:

- гарантированно повысится уровень информационной безопасности инфраструктуры предприятия;
- появляется объективная оценка качества программного обеспечения, имеющегося в организации;
- снижается риск по потери важной информации из-за внешних и внутренних уязвимостей.
- увеличиваются шансы по получению сертификата с первой попытки;
- сокращается время сертификации системы управления информационной безопасностью (СУИБ);
- повышается уровень доверия существующих клиентов и увеличивается клиентская база за счет привлечения новых клиентов;
- появляется возможность выхода на новые рынки благодаря наличию международных сертификатов;
- увеличивается отдача от инвестиций, которые вкладываются в безопасность корпоративных информационных систем [24, с. 83].

Этап внедрения мер информационной безопасности компании содержит следующие решения:

- осуществление защищенного доступа в сеть Интернет;
- обеспечение защиты от инсайдеров, а также утечек конфиденциальной безопасности (DLP-решения);
- обеспечение защиты корпоративного интернет-портала и сайта e-Commerce;
- наличие подсистемы антивирусной защиты и защиты от спама;

- создание решения для сокрытия или защиты конфиденциальной информации компании от несанкционированного доступа;
- наличие защищенного взаимодействия с мобильными работниками компании, которые осуществляют свою рабочую деятельность вне офиса;
- наличие защищенного доступа партнеров компании к ее корпоративным ресурсам;
- создание защищенного взаимодействия с клиентами компании;
- защита и шифрование корпоративной почты компании;
- защита локальной и беспроводной сети;
- защищенность IP-телефонии компании;
- возможность обнаружения и предотвращения вторжений и сетевых атак на информационные и сетевые ресурсы компании;
- наличие сертификатов и электронной цифровой подписи в компании;
- наличие возможностей для расширенной («строгой») аутентификации пользователей в сети;
- использование смарт-карт [9].

Для эффективного управления информационной безопасностью компании после того как внедрена ИБ-система необходима соответствующая техническая поддержка решений и своевременного постпроектного консалтинга, поэтому в рамках этапа поддержки рекомендуется использование:

- системы мониторинга и составления отчетности пользования информационными ресурсами в компании;
- технической поддержки и сопровождения систем информационной безопасности;
- обучения специалистов компании в области информационной безопасности [34].

Классическим представлением оценки вероятности реализации угрозы информационной безопасности современной компании, является оценка угроз, уязвимостей и ущерба, который могут нанести при их реализации.

При оценке вероятности реализации угроз необходимо опираться на известную статистику возникновения аналогичных инцидентов безопасности в прошлом. Вероятность реализации угроз определяется при помощи экстраполяции имеющихся данных. Как показывает практика, полученные значения чаще всего интерпретируется при помощи дискретной шкалы.

Проведение оценки уязвимостей необходимо для того, чтобы определить каким иммунитетом должны обладать компоненты инфраструктуры к выявленным угрозам. Данную оценку можно сформировать на основе совокупности сведений, собранных в компании о наличии имеющихся качественных и количественных известных технических ошибок и недоработок, найденных в защищаемой системе.

При проведении оценки ущерба необходимо включить в себя не только калькуляцию прямых убытков вследствие реализации угроз, но и степень нанесенного ущерба в диапазоне от незначительного до высокого.

Данный подход только на первый взгляд кажется простым, но на практике при вычислении рисков можно натолкнуться на различные проблемы, из которых можно выделить недостаточность сведений:

- о едином стандарте и его классификации;
- об известных компании угрозах безопасности;
- о качественной оценке уязвимостей;
- о системах технической экспертизы.

В сложившейся ситуации можно сделать вывод, что в подавляющем большинстве случаев процесс, связанный с управлением информационной безопасностью основывается на оценке рисков, которые существуют при принятой политике безопасности современной компании и с учетом имеющихся у нее средств защиты. При этом некоторые риски, которые связаны с

недостаточной надежностью элементов информационной системы, могут не учитываться в результате отсутствия достоверных данных.

В результате компаниям приходится нести расходы, для того чтобы снизить вероятность осуществления известных рисков, а неизвестные риски так и остаются за рамками внимания. Применительно к формуле оценки рисков можно говорить об отсутствии достаточных сведений об уязвимостях при определенных угрозах и ущербе.

Основой модели управления информационной безопасностью в компании является база знаний, которая содержит исчерпывающие сведения об известных угрозах информационной безопасности, а также демонстрировать связь этих брешей с возможностью реализации конкретной угрозы. Кроме того, в базе знаний должны содержаться сведения о принятой классификации опасности уязвимостей, а также указания на методику оценки влияния специфики информационного окружения.

При изучении существующих решений, необходимо рассмотреть классические системы управления уязвимостями, основной задачей которых является предоставление администратору информационной безопасности удобных инструментов по выявлению, сопровождению и устранению известных проблем безопасности в информационных системах.

Несмотря на хорошую реализацию модели управления жизненным циклом уязвимостей, данные системы имеют ограниченные возможности по выявлению этих брешей. Обычно, основным инструментом аудита является сканер безопасности, который предназначен лишь для того чтобы выявить активные уязвимости безопасности, которые можно эксплуатировать напрямую. Но как показывает практика, наибольшей угрозой являются пассивные уязвимости, которые могут проявиться лишь в случае совокупного воздействия нескольких внешних и внутренних факторов.

При исследовании методов оценки информационной безопасности компании, можно обратиться к стандарту по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

Этот стандарт определяет требования по проведению регулярных внешних и внутренних оценок информационной безопасности, а также самооценки информационной безопасности.

Основной целью методики, которая предлагается в рассматриваемом стандарте является стандартизация подходов и способов оценки соответствия обеспечения информационной безопасности компании требованиям по следующим направлениям:

- оценка текущего уровня информационной безопасности компании;
- оценка менеджмента информационной безопасности компании;
- оценка уровня осознания информационной безопасности компании [27].

Основными задачами данной методики являются следующие:

- определить состав показателей информационной безопасности и способов их оценивания;
- определить способ оценивания текущего уровня информационной безопасности компании, при помощи установления степени выполнения требований;
- определить способ оценивания менеджмента информационной безопасности современной компании и уровня осознания информационной безопасности при помощи установления степени выполнения требований,;
- определить итоговый уровень соответствия информационной безопасности компании требованиям [27].

Для того чтобы провести оценку степени соответствия информационной безопасности компании требованиям политике безопасности организации нужно использовать групповые и частные показатели информационной безопасности.

При групповых показателях информационной безопасности образуется структура направлений оценки, детализирующая оценку текущего уровня информационной безопасности компании, менеджмента и уровня осознания информационной безопасности.

Частные показатели информационной безопасности современной компании входят в состав групповых показателей и представляются в виде вопросов, ответы на которые могут дать возможность в определении оценок, которые затем формируют оценки групповых показателей.

Частные показатели можно разделить на две основные категории. В первую категорию входят частные показатели, которые отражают требования, выполнение которых является обязательным для компании. Вторую категорию составляют частные показатели, которые отражают положения, выполнение которых необходимо для компании [15, с. 55].

Оценку текущего уровня информационной безопасности компании можно определить с помощью следующих групповых и частных показателей информационной безопасности:

- ИБ в случае назначения и распределения ролей и обеспечении доверия к сотрудникам компании;
- ИБ в случае управления доступом и регистрацией;
- ИБ при помощи средств антивирусной защиты;
- ИБ в случае использования Интернет-ресурсов;
- ИБ в случае использования средств криптографической защиты информации;
- ИБ для информационных и платежных технологических процессов;
- обработка персональных данных в организации;
- ИБ технологических процессов, в рамках которых производится обработка персональных данных [3].

Оценка менеджмента информационной безопасности компании определяется при помощи групповых и частных показателей информационной безопасности, которые позволяют провести оценку степени выполнения требований информационной безопасности для следующих задач:

- организовать функционирование службы информационной безопасности компании;

- определить и изменить в случае необходимости область действия системы обеспечения информационной безопасности;
- выбрать и изменить подходы к оценке рисков нарушения информационной безопасности и провести оценку рисков нарушения информационной безопасности;
- разработать планы обработки рисков нарушения информационной безопасности;
- разработать и провести коррекцию внутренних документов компании, которые регламентируют ее деятельность в области обеспечения информационной безопасности;
- принять руководством компании решение о реализации и эксплуатации систем обеспечивающих информационную безопасность компании;
- организовать и реализовать планы по обработке рисков нарушения информационной безопасности;
- разработать и организовать реализацию программ, связанных с обучением и повышением осведомленности в области информационной безопасности;
- организовать своевременное обнаружение и реагирование на инциденты информационной безопасности;
- организовать обеспечение непрерывности бизнеса и его восстановление после прерываний;
- провести мониторинг информационной безопасности компании и контролировать существующие защитные меры;
- провести самооценку информационной безопасности компании;
- провести внешний аудит информационной безопасности;
- проанализировать функционирование системы обеспечения информационной безопасности компании;
- проанализировать систему обеспечения информационной безопасности компании со стороны руководства;

- принять решения по тактическим улучшениям системы обеспечения информационной безопасности компании;
- принять решения по стратегическим улучшениям системы обеспечения информационной безопасности компании [4].

Результат проведения оценки формируется на основе аудиторского заключения в случае проведения оценки соответствия внешней организацией или отчета самооценки в случае если оценка соответствия проводилась силами организации БС РФ.

В Федеральном Законе от 27.12.2002 № 184-ФЗ «О техническом регулировании» установлены рекомендации стандартов, а также других документов по стандартизации, которые в свою очередь подлежат обязательному исполнению в компаниях, в случае добровольного принятия решения о присоединении [2].

Подводя итог вышесказанному, можно отметить тот факт, что современные средства по управлению уязвимостями являются несовершенными, поэтому к вопросам защиты информации необходимо подходить комплексно, объединяя организационные, программные и аппаратные методы защиты.

Анализ теоретической части дипломной работы показал, что на сегодняшний момент для предприятий существует большое количество угроз информационной безопасности, которые можно подразделить на две большие группы — внутренние и внешние угрозы.

Внутренние угрозы информационной безопасности создают сотрудники предприятия — инсайдеры, в зависимости от действий которых предприятие может понести тот или иной ущерб.

Внешние угрозы осуществляются злоумышленниками вне компании по техническим каналам связи.

Для предотвращения угроз или их минимизации необходимо использовать организационные методы, а также программно-аппаратные системы для предотвращения рисков, связанных с утечкой ценных данных, из-за которых предприятие может понести серьезные финансовые потери.

1.3 Анализ защиты информации общества с ограниченной ответственностью «Нэт Бай Нэт Холдинг»

1.3.1 Характеристика и организационная структура общества с ограниченной ответственностью

ООО «Нэт Бай Нэт Холдинг» — российская телекоммуникационная компания, более 20 лет предоставляет услуги связи частным и корпоративным пользователям, в том числе услуги широкополосного доступа в Интернет, цифрового телевидения, виртуального хостинга, системной интеграции [22].

На рисунке 4 приведена организационная структура управления

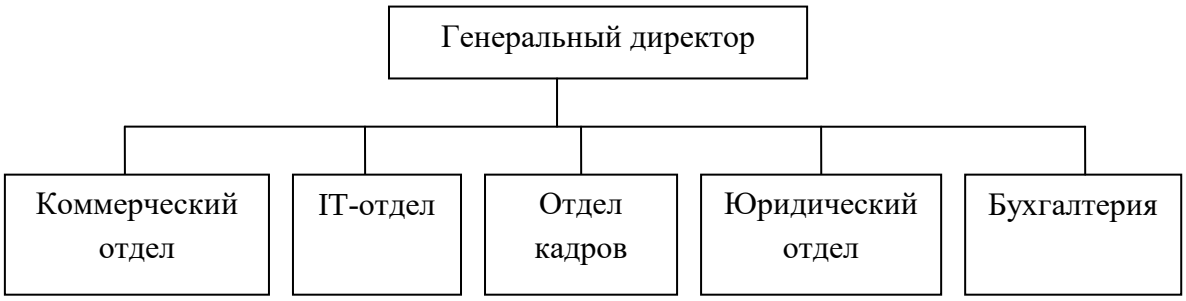


Рисунок 4 — Организационная структура управления предприятия

Возглавляет ООО «Нэт Бай Нэт Холдинг» генеральный директор, ему в свою очередь подчиняются руководители отделов по направлениям. В обязанности директора входит организация и управление имуществом, определение организационной структуры предприятия и утверждение штатного расписания, поощрение и наказание подчиненных работников, а также другие вопросы, связанные с управлением.

Руководитель, исходя из принципа «кадры решают все», ведет работу по удовлетворению требований и ожиданий персонала, наделяет перспективных, по его мнению, сотрудников дополнительными полномочиями показывая при этом перспективу продвижения по службе.

По решению руководителя приоритет в продвижении по службе отдается молодым и перспективным сотрудникам компании, которым дается возможность проявить себя, показать свои умения в наибольшей степени, тем самым привязывая специалистов к организации.

Подводя итог, можно сказать, что генеральный директор осуществляет общее руководство компанией и решает ее стратегические вопросы.

Охарактеризуем основные структурные подразделения ООО «Нэт Бай Нэт Холдинг» — отдел внедрения, IT-отдел, бухгалтерия, юридический отдел и отдел кадров.

Коммерческий отдел состоит из нескольких бюро, каждое из которых осуществляют свою деятельность согласно нескольким направлениям — продажи, внедрение, сопровождение. Во главе каждого бюро находится начальник, отвечающий за координацию и контроль за деятельностью специалистов своего направления. В обязанности специалистов по продажам входит продвижение и продажа услуг связи. У специалистов по эксплуатации основной задачей является обеспечение бесперебойного предоставления услуг.

Бухгалтерия готовит различные финансовые документы — счета-фактуры, накладные на сторону, документы на запросы налоговых органов и других организаций, а также ведет учет заработной платы. Бухгалтерия осуществляет учет текущих финансовых операций, доходов и расходов компании, основных и оборотных средств компании.

Отдел кадров ООО «Нэт Бай Нэт Холдинг» осуществляет прием и увольнение сотрудников, а также их перемещение внутри компании, совместно с генеральным директором разрабатывает штатное расписание» и систему мотивации и стимулирования труда. Отдел кадров принимает участие в собраниях трудового коллектива, являясь представителем его интересов. При необходимости осуществляет организацию профессионального обучения работников, необходимых компании.

Юридический отдел осуществляет проверку соответствия требованиям законодательства представляемых на подпись руководителю договоров, проектов приказов, инструкций положений и других документов правового характера. Представляет в установленном порядке интересы ООО «Нэт Бай Нэт Холдинг» в суде, арбитраже, а также в других органах при рассмотрении правовых вопросов.

Динамика показателя среднемесячной заработной платы за последние три года в ООО «Нэт Бай Нэт Холдинг» свидетельствует о росте данного показателя, что связано с ростом уровня жизни населения. Так среднемесячная заработная плата высшего звена выросла с 50 256 руб. в 2017 году до 70 000 руб. в 2018 году. Среднемесячная заработная плата среднего звена 2018 году выросла по сравнению с 2017 годом почти в 2 раза и составила 46 250 руб. Среднемесячная заработная плата остального персонала выросла не сильно и на данный момент составляет 30 000 руб.

Компания в последнее время встала перед проблемой защиты конфиденциальной информации. В последнее время участились случаи установки программных продуктов и обновлений к ним, поставляемой данной компанией своим клиентам у других клиентов.

В связи с этим компании необходимо провести анализ угроз и рисков для того чтобы найти недостатки в защите информации и устранить потенциальные «дыры» в системе защиты.

1.3.2 Оценка состояния информационной безопасности на предприятии

На предприятии ООО «Нэт Бай Нэт Холдинг» существует 2 сети: открытая и закрытая. В открытой сети находятся компьютеры с интернетом, и компьютеры подразделений неработающих с конфиденциальными данными. В закрытой сети подключены компьютеры, на которых храниться или работают с закрытой (секретной и конфиденциальной) информацией.

Так же в ООО «Нэт Бай Нэт Холдинг» идет постоянный обмен данными с клиентами компании, с которыми осуществляется обмен информацией и обновлениями к программным продуктам. С контрагентами ведутся постоянные разговоры по телефону (разбор ошибок, различные уточнения, поправки и другая информация), пересылка электронных писем по e-mail, а также прием и отправка документов по факсу.

Офис ООО «Нэт Бай Нэт Холдинг» состоит из пяти комнат. Там имеется 13 компьютеров и 2 сервера. Также имеется ряд вспомогательных комнат на прямую не относящихся к деятельности компании (туалет, кухня, балкон, он же комната для курения).

Их соединяет единая информационная система, на базе локальной сети типа «звезда», с использованием одного 24 портового коммутатора Ethernet, фирмы-производителя Dlink, с пропускной способностью 1 Гбит/с.

Он является неуправляемым коммутатором 1-Гбит/с предназначенным для повышения производительности работы малой группы пользователей, обеспечивая при этом высокий уровень гибкости.

Мощный и, одновременно с этим, простой в использовании, Dlink позволяет пользователям без труда подключить к любому порту сетевое оборудование, работающее на скоростях 1 Гбит/с, понизить время отклика и удовлетворить потребности в большой пропускной способности сети).

В качестве сетевого оборудования в ПК используются либо интегрированные варианты, либо сетевые карты D-Link DFE-520TX 1Gbps, восьмижильного кабеля (витая пара).

Техническая архитектура, состав и взаимодействие аппаратных средств, используемых для обработки информационных активов, подлежащих защите, изображена на рисунке 5.

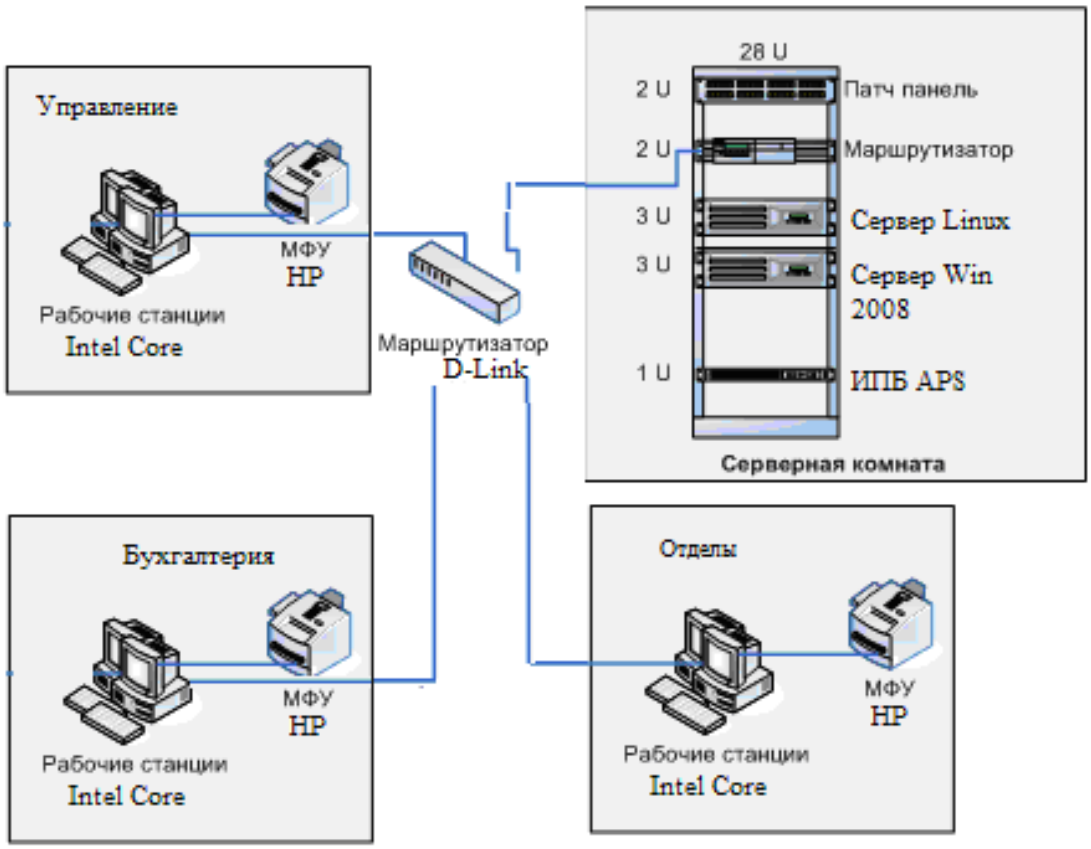


Рисунок 5 — Техническая архитектура компании

Имеющиеся на предприятии два сервера работают под разными операционными системами: один под управлением ОС Linux, а другой под управлением Microsoft Windows 2008 Server.

В качестве сервера используются системы на основе процессора Intel Xeon, обладающие характеристиками, представленными в таблице 3.

Таблица 3 — Конфигурация одного из серверов

Процессор	Intel Xeon 5500
Оперативная память	12 Гб DDR3 Samsung
Дисковая память	1 Тб x 2 RAID Edition SATA , RAID массив
Резервное копирование	Зеркальное, посредством RAID
Видео подсистема	GeForce nVidia 7600GS
Операционная система	Windows Svr 2008

Каждый из серверов служит шлюзом для выхода в интернет. Windows сервер является основным выходом в интернет (Hi-max), Linux сервер же в свою очередь является резервным выходом в интернет (turbo- интернет). В данной локальной сети используется диапазон IP-адресов 192.168.1.0 —

192.168.1.24. Причем: 192.168.1.1 — Linux server; 192.168.1.2 — Windows server.

В качестве базовых технических средств по оснащению корпоративной сети применяются следующие средства вычислительной техники (СВТ).

Таблица 4 — Конфигурация рабочих станций

Процессор	Intel I3 1,8
Оперативная память	4096 Мб
Дисковая память	500 Гб
Видео подсистема	интегрированные решения
Операционная система	Windows 7 SP 2

Все рабочие места состоят из стандартного набора: ЖК-монитор, системный блок, клавиатура и мышь. В торговом зале и группе ПО расположены два сетевых лазерных принтера (многофункциональный Cannon MF3110 и Canon Laser Shot LBP1120). Доступ к Интернету осуществляется через сервер. В офисе имеется три телефонных линии, на двух из них установлен факс.

На каждую из рабочих станций установлена ОС семейства Windows, преимущественно это Windows 7 и Windows 10. Также на некоторые компьютеры были установлены следующие программные продукты:

- Kaspersky Internet Security предназначена для того чтобы в реальном времени предоставлять защиту персональных компьютеров от различных вирусных программа так же иных современных угроз.
- программные продукты 1С, предназначенные для ведения бухгалтерского, налогового, управленческого, торгового и складского учетов.

Среди программных продуктов по регламентированному учету можно выделить:

- 1С: Бухгалтерия 8.3;
- 1С: Зарплата и управление персоналом 8.

По торговому и складскому учету можно выделить продукты:

- 1С: Управление Торговлей;
- 1С: Розница 8.

По управленческому учету выделим:

- 1С: ERP Управление предприятием;
- 1С: Документооборот (СЭД);
- 1С: Управление корпоративными финансами.

MS Office, который является офисным пакетом приложений, который создала корпорация Microsoft, состоящий из программного обеспечения, предназначенного для работы с различными документами — это могут быть тексты, электронные таблицы, базы данных и др. Microsoft Office имеет встроенные OLE-объекты, связи с чем его функции могут использовать другие приложения.

На сервере ООО «Нэт Бай Нэт Холдинг» установлены сетевые программы от российской компании 1С. К данным программам существует доступ с других рабочих станций, безопасность настроена таким образом, что сотрудник может войти в программу только под своими учетными данными, это сделано для того, чтобы у каждого был соответствующий набор прав. Кроме того, в ООО «Нэт Бай Нэт Холдинг» есть файл-сервер, на котором находятся реестры документооборота, договора, а также другие необходимые компании документы. Тут же находится дистрибутив с обновлениями и пополнениями для разного программного обеспечения компании. В отличие от рабочих станций за файл-сервером никто не работает, он является «архивом» или «хранилищем» важных данных для компании. Права администратора на файл-сервере имеются только у руководителя IT-отдела и системного администратора.

Так же на предприятии расположен собственный Web-Сервер с размещенным на нем сайтом предприятия. Этот сервер помимо сайта осуществляет раздачу интернета по средствам прокси-сервера на некоторые компьютеры в открытой сети, а также обеспечивает работу почтового клиента MS Outlook. Сервер еще осуществляет обновление баз данных антивируса.

Самыми важными информационными ресурсами компании, которые необходимо защищать наиболее тщательно являются лицензии к программным продуктам 1С, дистрибутивы программ, а также обновления к ним.

Коммерческую тайну ООО «Нэт Бай Нэт Холдинг» составляет финансово-экономическая информация, а также база данных клиентов и поставщиков компании и переписка с ними.

Персональные данные ООО «Нэт Бай Нэт Холдинг» составляет информация о сотрудниках компании, такая как паспортные данные, страховые данные, сведения о доходах, сведения о семейном положении и т.п.

1.4 Электронные образовательные ресурсы

Электронный образовательный ресурс (ЭОР) — это ресурс, представленный в электронно-цифровой форме и включающий в себя структуру, предметное содержание и метаданные о них (ГОСТ 52653-2006), иначе говоря это учебные материалы, для воспроизведения которых используются электронные средства.

На данный момент, образовательный процесс тяжело представить без использования ЭОР, которые в той или иной мере присутствуют в сфере обучения. Школьники и студенты выполняют домашние задания и работы при помощи компьютеров и сети интернет, уроки в учебных заведениях проводятся при помощи интерактивных досок и проекторов. Также большое количество занятий проводится дистанционно посредством веб- трансляций. Преподаватель может на расстоянии проводить занятия с учениками, посредством сети интернет и получать от обучающихся обратную связь.

Михалищева М. А. в своей статье пишет о том, что электронное пособие — это не электронный вариант книги, функции которой ограничиваются возможностью перехода из оглавления по гиперссылке на искомую главу. В зависимости от вида изложения (лекция, семинар, тест, самостоятельная работа) сам ход занятия должен быть соответствующим образом адаптирован

для достижения эффекта от использования такого пособия, а само пособие должно поддерживать те режимы обучения, для которых его используют. [12]

Как правило, электронные учебные пособия строятся по модульному принципу и включают в себя текстовую часть, графику (статические схемы, чертежи, таблицы и рисунки), анимацию, натурные видеозаписи, а также интерактивный блок. Использование компьютерной анимации позволяет визуализировать сложные схемы, процессы и явления макро- и микромира, заглянуть внутрь уникального оборудования. Все это делает учебный процесс увлекательным, ярким и в конечном итоге более продуктивным.

В большой степени возможности электронных учебных пособий раскрываются при самостоятельной работе. Здесь могут оказаться востребованными все мультимедийные функции: анимация и видео, интерактивные компоненты, вовлекающие обучаемого в учебный процесс и не дающие ему отвлечься, дикторский голос и подобранное музыкальное сопровождение, и все возможности компьютерной поисковой системы. [14]

Титова Е. И. в своей статье описывает создание электронных учебников. Рассматривает средства, используемые при создании учебников. Выделяет этапы, на которые следует опираться. Электронные учебники могут иметь различную структуру: линейную, древовидную, фреймовую.

Средства создания электронных учебников можно разделить на группы на основе комплексного критерия, учитывающего назначение и выполняемые функции, требования к техническому обеспечению и особенности использования. В соответствии с этим критерием можно выделить следующие классы [33]:

- традиционные алгоритмические языки;
- инструментальные средства общего назначения;
- средства мультимедиа;
- гипертекстовые и гипермедиа средства.

При создании электронных образовательных ресурсов выделяют следующие принципы:

1. Наглядность. Наглядность обучения построена на важнейших моделях восприятия информации (зрение, слух), именно при их использовании происходит более эффективное обучение, позволяя собрать максимум наглядности в виде аудио, фото, видео – материалах, и других видах мультимедийной информации, что улучшает восприятие и повышает процент запоминаемой информации.

2. Интерактивность. Во время занятий учащийся должен выполнить какие- либо интерактивные действия: просмотр видеоролика, либо прослушивание учебной аудиозаписи, воспользоваться элементами навигации, пройти тестирование или ответить на вопросы по теме урока.

3. Практическая часть. Для всего теоретического материала должен иметься блок практических заданий, будь то учебные задачи, тестовые вопросы, лабораторные работы.

4. Доступность. Изложение материала должно быть постепенным, от простого по нарастающей к сложному.

5. Научность изложения материала. Содержание курса должно опираться на обоснованной, достоверной и признанной информации.

6. Последовательность изложения. Логическое содержания курса даёт возможность преподавать либо вести самообучение как последовательное и постепенное, либо опережающее или повторяющее норму. Диалоговые сообщения и гипертекстовые ссылки позволяют переходить к уже пройденной теме, либо перейти к теме, которую ещё предстоит пройти.

7. Модульность и вариативность изложения. Материал структурирован на темы и под темы. Структура позволяет выстраивать процесс обучения индивидуально, вариативно, в зависимости от задач обучения.

2 ОПИСАНИЕ ЭЛЕКТРОННЫХ ИНСТРУКЦИЙ ПО ЗАЩИТЕ ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

2.1 Структура

Опираясь на рассмотренные статьи по структуре электронных инструкций выделим следующие разделы:

- теоретическую часть, в основе данной части содержится текст, графика (статические схемы, чертежи, таблицы и рисунки), анимация, натурные видеозаписи, а также интерактивный блок;
- практическая часть, там должно быть представлено пошаговое решение типичных задач и упражнений по данному учебному курсу с содержанием минимальных пояснений;
- контрольная часть — содержит набор тестов, контрольных вопросов по теоретической части, но так же и решение задач и упражнений по практике.

На основе данной схемы разработаем электронные инструкции

Инструкции разработаны для сотрудников ООО «Нэт Бай Нэт Холдинг». Каждый вновь принимаемый сотрудник, проходя обходной лист в отделе безопасности знакомится с правилами безопасности, которые он должен соблюдать при работе с компьютером в локальной сети компании ООО «Нэт Бай Нэт Холдинг».

Данные инструкции могут быть использованы всеми сотрудниками, работающими с персональными компьютерами для того чтобы ознакомиться с правилами работы в сети, знать какое программное обеспечение запрещено устанавливать на рабочие компьютеры.

Сборник инструкций можно разделить на 3 блока:

- теоретический раздел;
- проверка знаний;

- практический раздел.

Теоретический раздел состоит из теоретического материала по работе в локальной сети, а так же политиками безопасности принятых на предприятии.

Практический раздел содержит инструкции по настройке оборудования, представленных как в текстовом виде, так и в виде видео-инструкций.

Проверка знаний содержит тесты и задания для определения уровня знаний по информационной безопасности у сотрудников предприятия (рисунок 6).

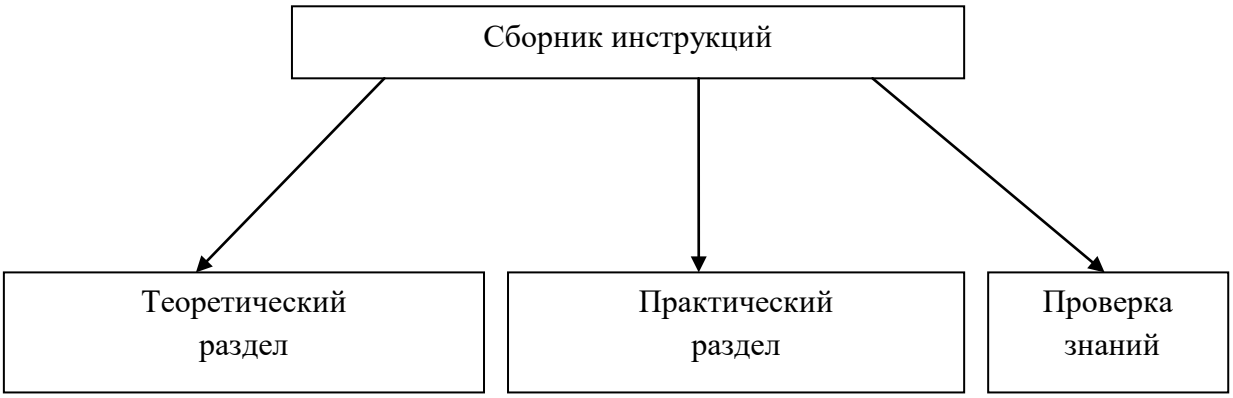


Рисунок 6 — Структура электронных инструкций

2.2 Описание навигации и интерфейса

Навигация представлена наличием основного меню перехода к рекомендациям обеспечения безопасности информации для сотрудников предприятия, а также наличием гиперссылок на бланки различных документов, связанных с безопасностью.

Электронные инструкции созданы с помощью редактора WIX и обычного блокнота.

Первое что нужно сделать при выборе интерфейса выбрать шаблон будущего методического пособия. Так как планируется создание веб-ресурса подразделения, отвечающего за безопасность, выбираем шаблон под тематику — безопасность.

Конструктор Wix довольно прост в использовании и имеет набор самых необходимых функций для успешного создания электронного методического пособия. В конструкторе предлагаются разработчику как платные, так и бесплатные варианты оформления. Стоимость платных шаблонов вполне демократична.

Далее приступаем к оформлению ресурса. После выбора подходящего шаблона нажимаем на кнопку «Редактор», после чего веб-мастер попадает в основное меню конструктора. Здесь можно привязать к веб-ресурсу собственное доменное имя и поменять любой элемент оформления, с помощью панели меню, расположенной в левой стороне страницы.

Для того чтобы дать название интернет сайту необходимо кликнуть в левом верхнем углу по значку в виде монитора. Мы зададим имя «Нэт Бай Нэт Холдинг» с логотипом компании соответствующее имени реальной компании (рисунок 7).

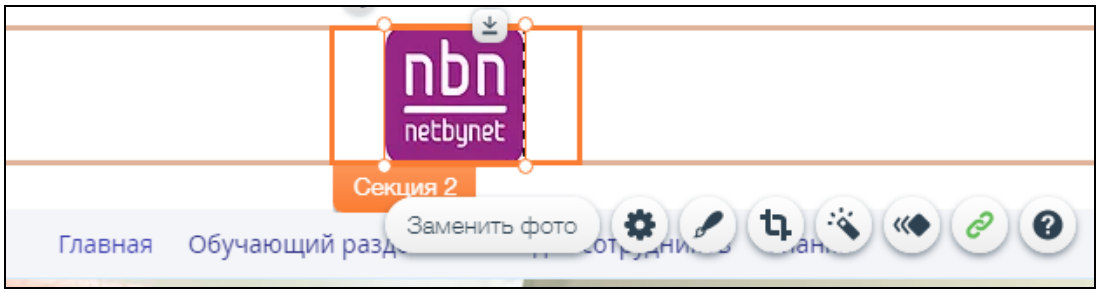


Рисунок 7 — Задание имени сайта

Конструктор сайтов Wix дает возможность добавления любых элементов на ресурс: кнопок социальных сетей, фотографий, галерей, статей и т. д. Очень просто поменять фон страницы. Далее добавим картинку, наименование электронного методического пособия, а также контакты сотрудников отдела безопасности для связи (рисунок 8).

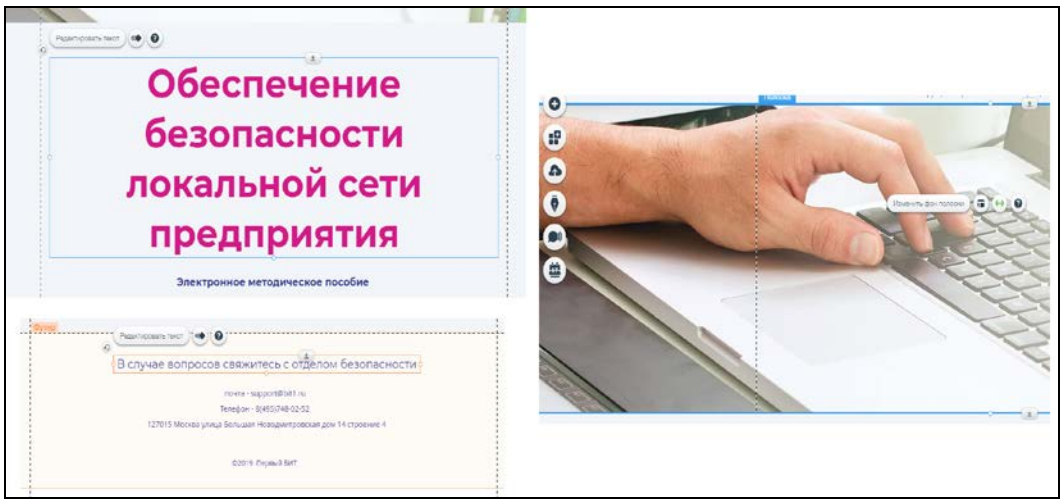


Рисунок 8 — Настройка главного меню

Управлять будем при помощи горизонтального меню. Меню состоит из четырех основных пунктов «Главная», «Теоретический раздел», «Практический раздел» и «Проверка знаний» (рисунок 9).

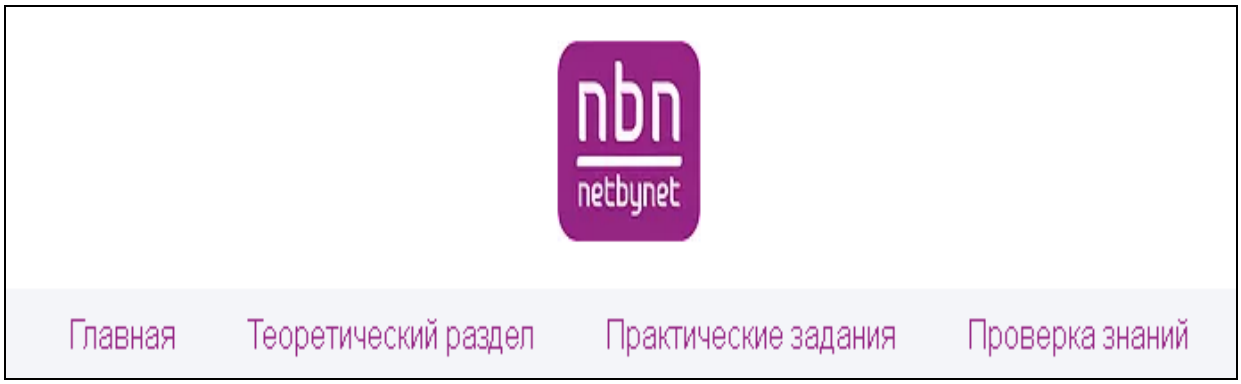


Рисунок 9 — Меню сайта

При нажатии на эти пункты меню осуществляется переход к странице с нужной информацией. При нажатии на пункт меню «Главная» мы попадаем на главную страницу. При нажатии на пункт меню «Теоретический раздел» открываются ссылки на текст при нажатии, на которые производится переход на страницы с нужным контентом.

Для создания этих страниц заходим в конструктор и жмем «Добавить страницу» (рисунок 10).

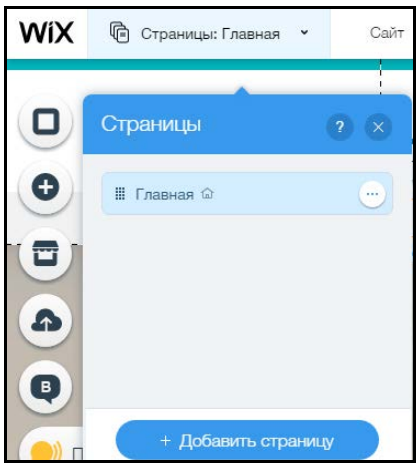


Рисунок 10 — Добавление новой страницы

В наименовании пишем «Теоретический раздел». Аналогично создаем еще три страницы «Теория», «Инструкция по работе в сети» и «Запрещенное ПО», которые обозначаем как субстраницы для обучающего раздела (рисунок 11).

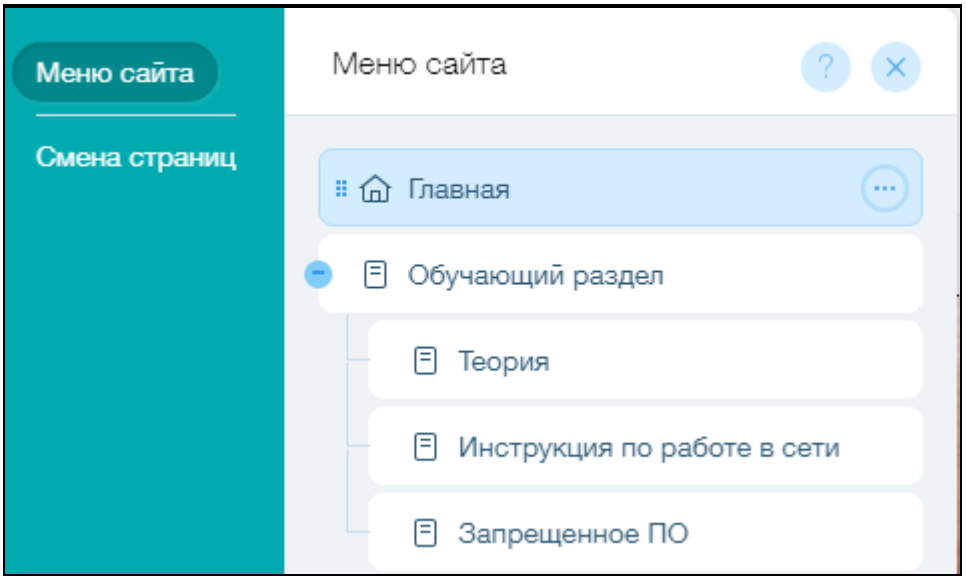


Рисунок 11 — Создание меню и подменю

Переходим на страницу «Инструкции по работе в сети» и наполняем ее контентом (рисунок 12) и пишем название страницы «О правилах поведения пользователей в корпоративной сети», в результате получаем страницу, наполненную необходимым контентом, в которой содержаться указания для пользователей о том, как нужно вести себя за компьютером в локальной сети.

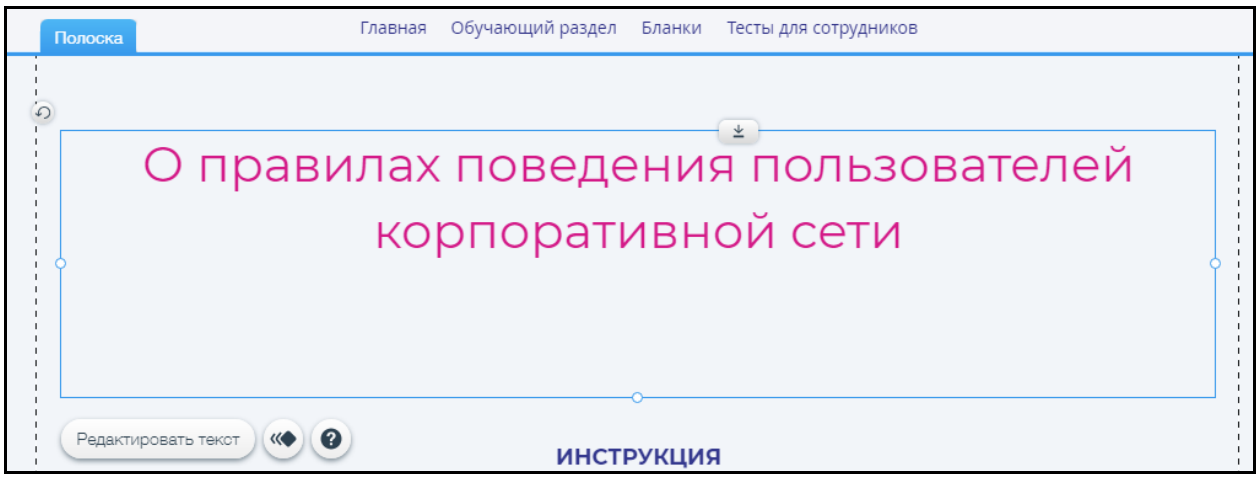


Рисунок 12 — Наполнение страницы контентом

Далее переходим на созданную страницу «Теоретический раздел», в которой будут содержаться теоретические материалы о защите информации на предприятии.

В наименовании пишем «Теоретический раздел» и делаем ссылку на пункт меню «Теоретический раздел». Наполняем данную страницу контентом и пишем название страницы «Теоретические основы защиты информации на предприятии», в результате получаем наполненную страницу (рисунок 13).

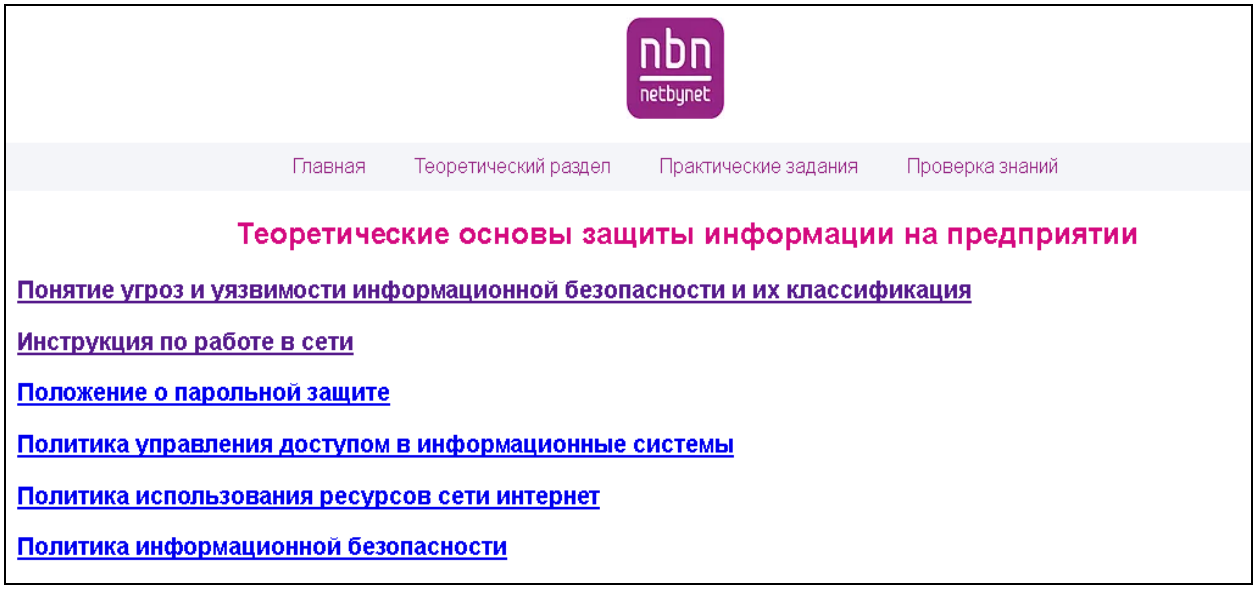


Рисунок 13 — Страница «Теоретический раздел»

Далее переходим на созданную страницу «Инструкция по работе в сети» в которой будут описываться программы, которые запрещены к использованию на компьютерах, входящих в корпоративную сеть.

В наименовании пишем «Инструкция по работе в сети» и делаем ссылку на пункт меню «Инструкция по работе в сети». Наполняем данную страницу контентом и пишем название страницы «Инструкция по работе в сети», в результате получаем наполненную страницу (рисунок 14).

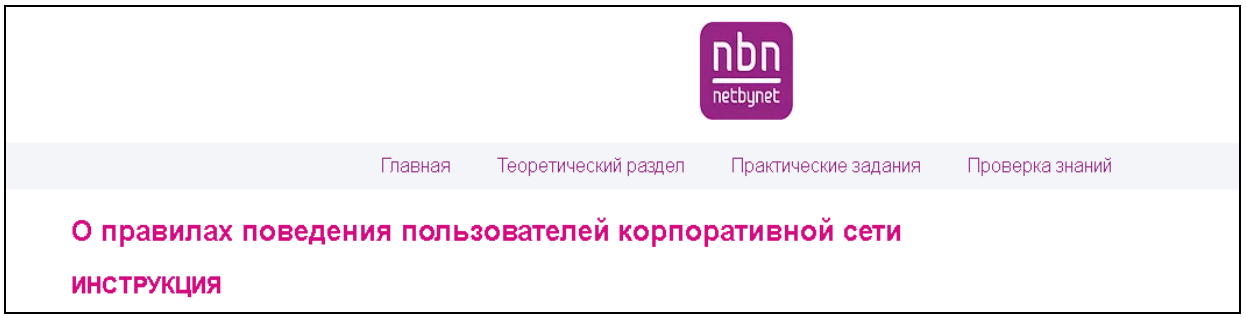


Рисунок 14 — Страница «Инструкция по работе в сети»

Далее создаем еще одну страницу «Проверка знаний» в которой будут содержаться задания, связанные с информационной безопасностью. Задания выполнены в виде тестов. Так же с помощью learning apps разработан кроссворд (рисунок 15).

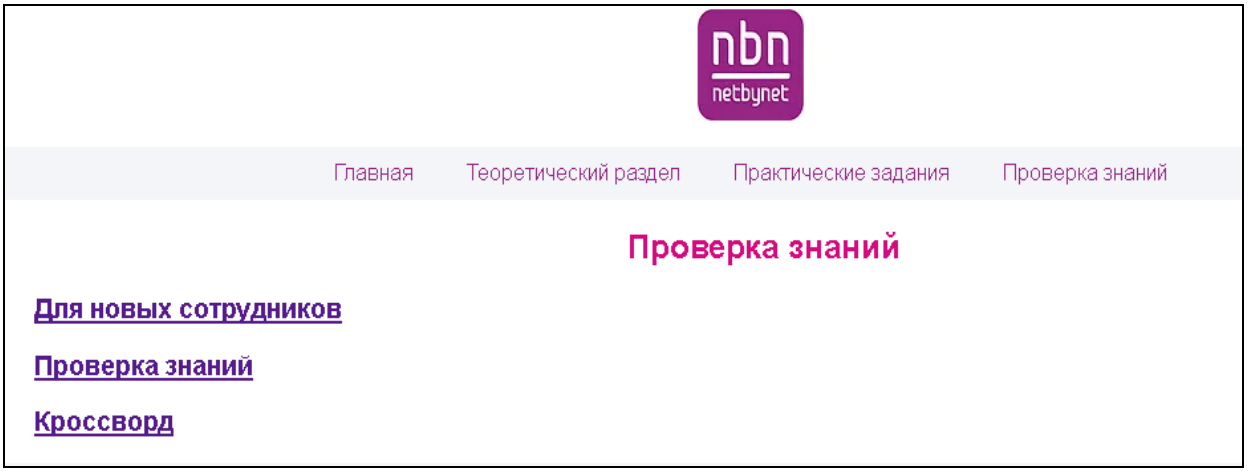


Рисунок 15 — Страница «Проверка знаний»

Далее создаем еще одну страницу «Практический раздел» в которой будут содержаться документы необходимые для обеспечения безопасности. Для создания этой страницы заходим в конструктор меню и жмем «Добавить страницу» (рисунок 10).

В наименовании пишем «Практический раздел» и делаем ссылку на пункт меню «Практический раздел». Наполняем данную страницу ссылками на контент с практическими заданиями (рисунок 16).

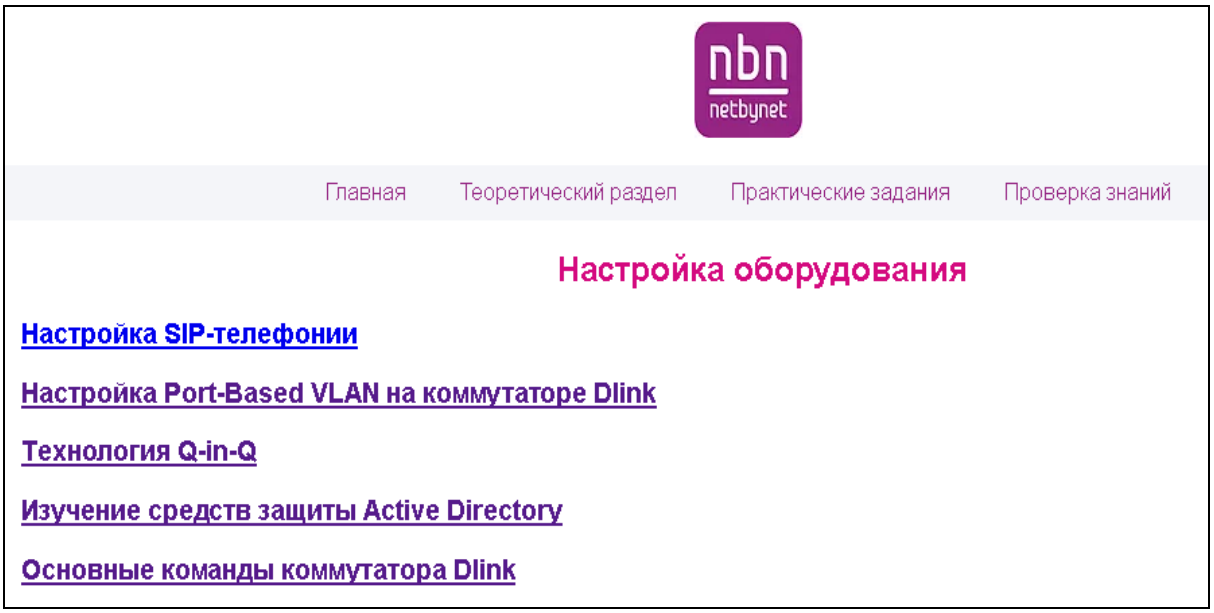


Рисунок 16 — Страница сайта «Практический раздел»

В качестве контента будут выступать файлы в формате текстовых страниц (рисунок 17).

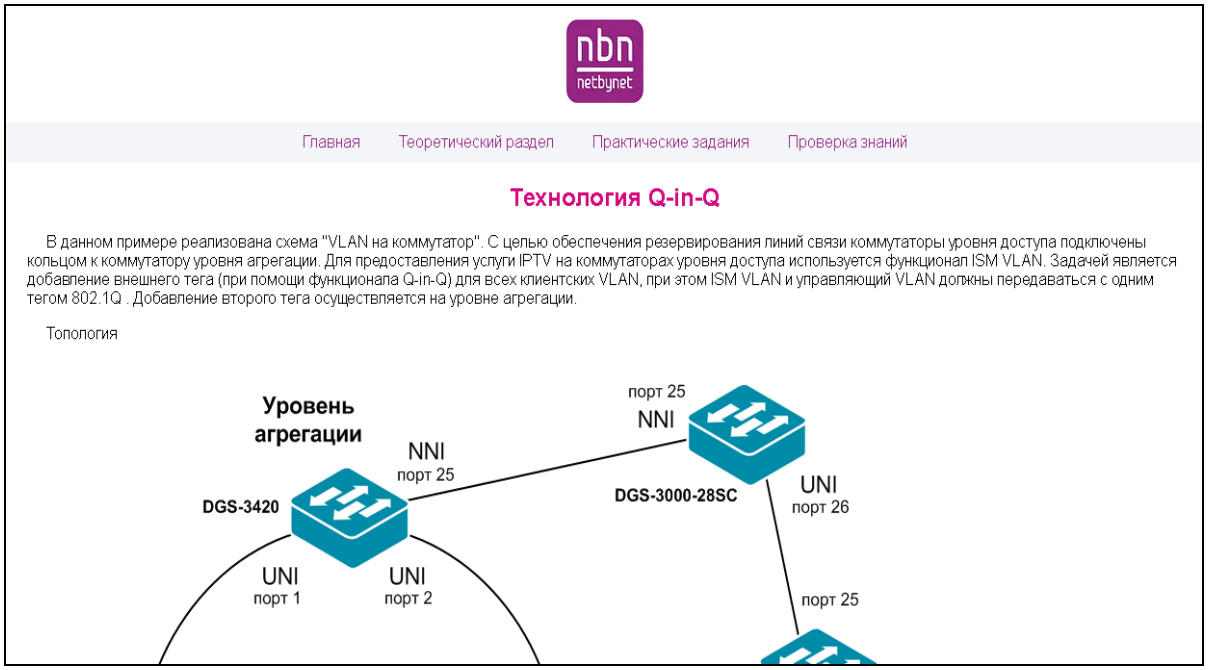


Рисунок 17 — Страница «Технология Q-in-Q»

А также добавлены видео-инструкции в дополнение к тексту (рисунок 18).

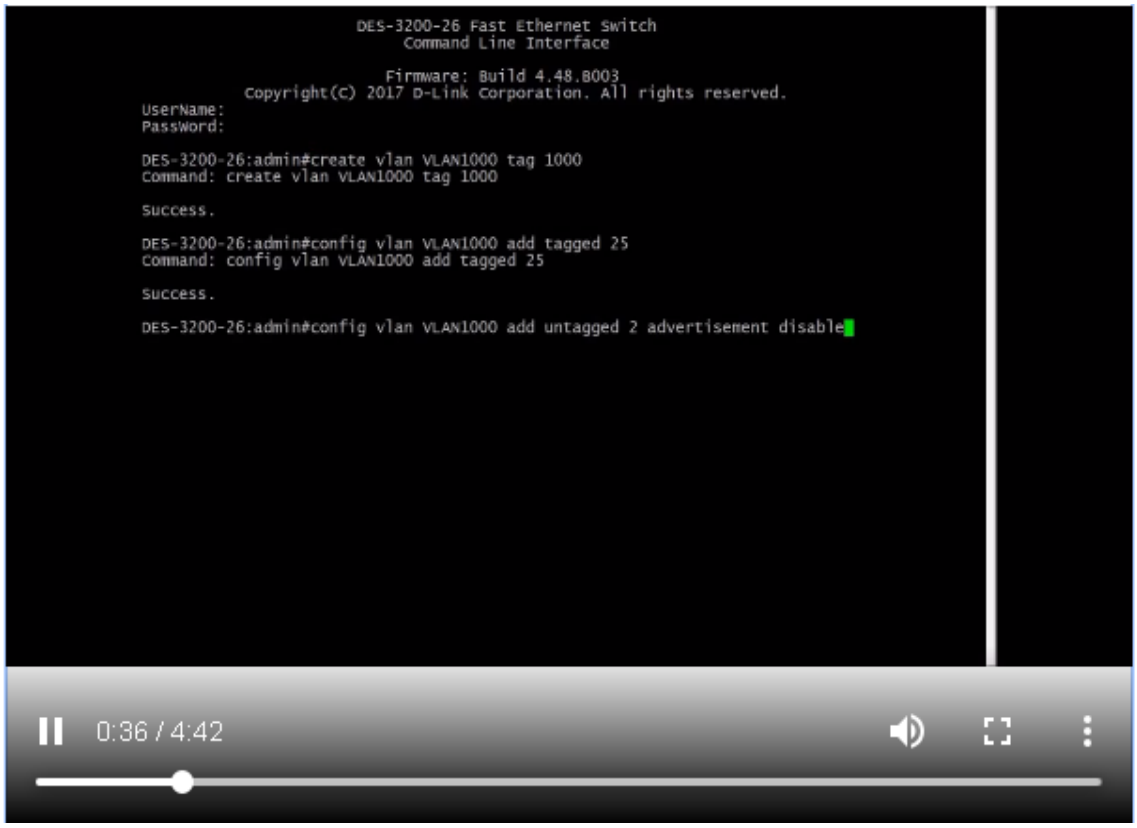


Рисунок 18 — Видео-инструкция «Технология Q-in-Q»

Далее сохраняем полученный результат (рисунок 19).

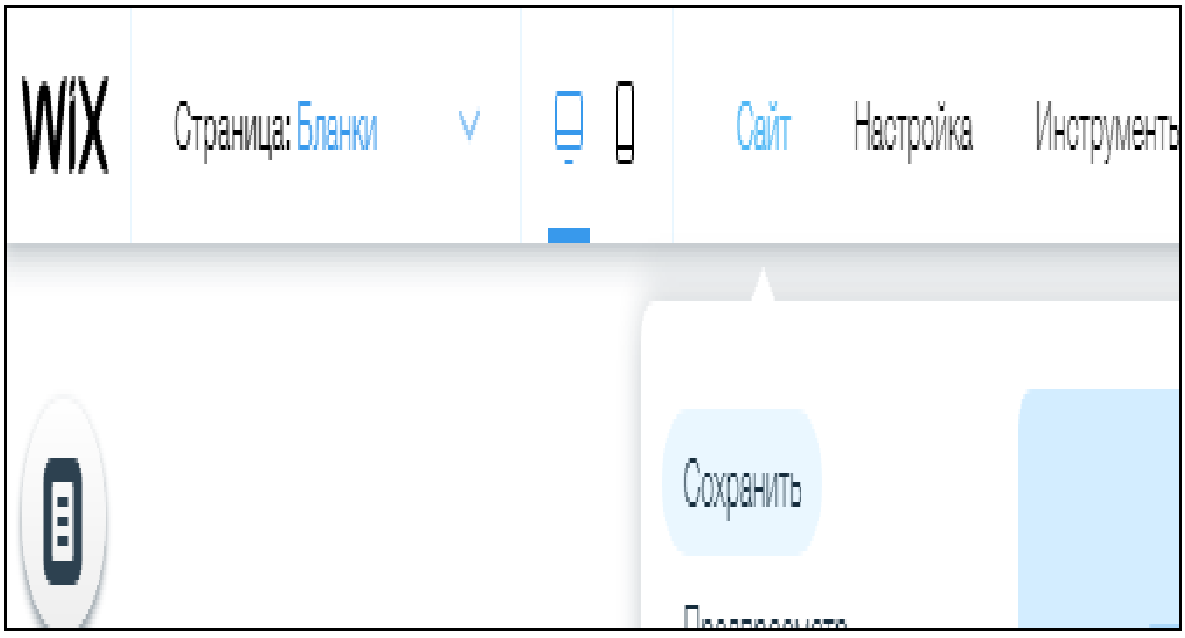


Рисунок 19 — Сохранение электронного методического пособия

Система сообщает о том, что все сделанные изменения будут сохранены, после публикации методическое пособие доступно для пользования.

Далее проведем тестирование разработанного электронного методического пособия.

2.3 Тестирование

Основное меню располагается в верхней части окна, под логотипом компании и содержит пункты, представленные на рисунке 20.

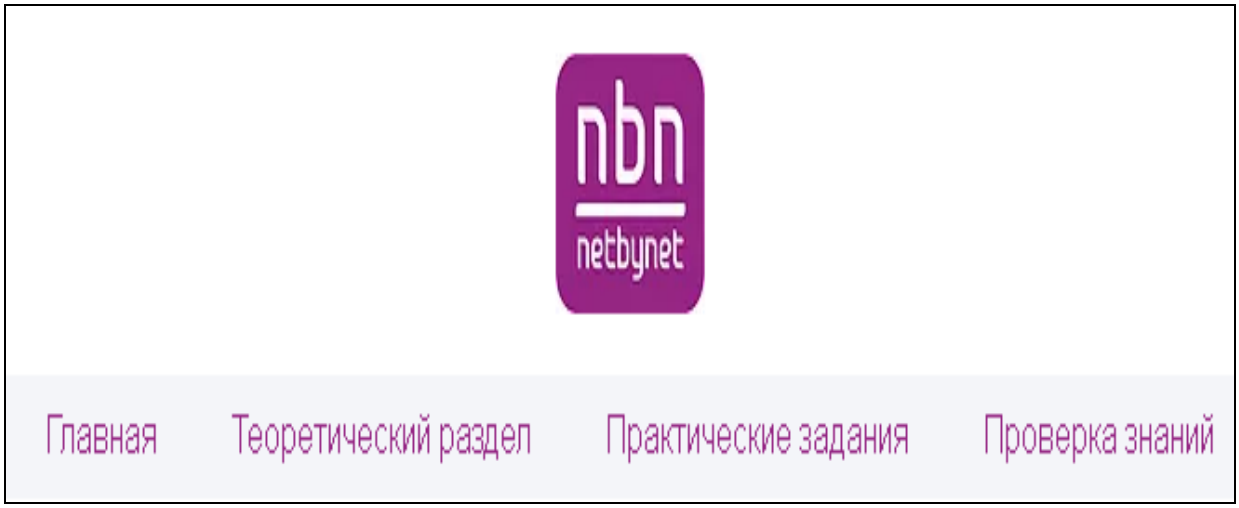


Рисунок 20 — Основное меню

Электронные инструкции состоят из логически связанных html-страниц, упорядоченных по смыслу. Основные страницы:

- главная
- теоретический раздел
- практические задания
- проверка знаний

В методическом пособии управление осуществляется через пункты основного меню, а также через гиперссылки.

В каждом разделе есть ссылки на определённый контент.

Главная страница (index.htm) приведена на рисунке 21 и содержит название и реквизиты для связи с отделом безопасности в случае вопросов, ответы на которые не были найдены на сайте.

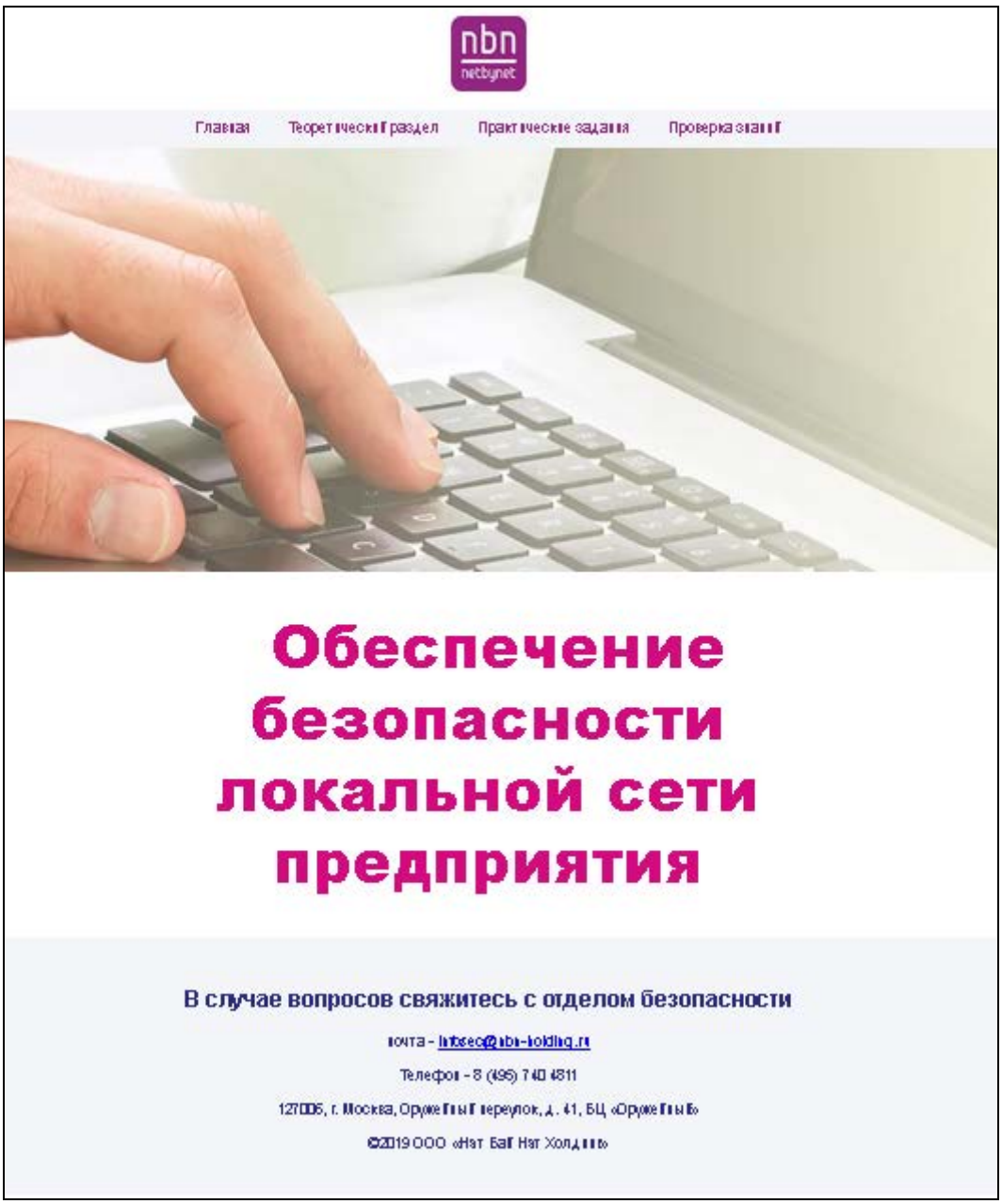


Рисунок 21 — Стартовая страница

Как видно из рисунка 21 электронные инструкции «Обеспечение безопасности локальной сети предприятия» включают в себя разделы:

- главная;
- теоретический раздел;
- практические задания;
- проверка знаний.

Теоретический раздел в свою очередь состоит из двух подменю «Инструкция по работе в сети» и «Запрещенное ПО» (рисунок 22).

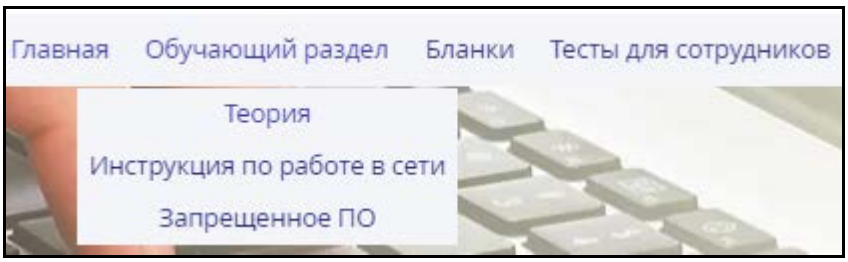


Рисунок 22 — Система подменю обучающего раздела

Раздел «Теория» включает в себя два теоретических материала на темы «Системы и методы защиты корпоративной информации от внутренних и внешних угроз» и «Понятие угроз и уязвимости информационной безопасности и их классификация» (рисунок 23).

При нажатии на кнопку скачать происходит скачивание файла с теоретическим материалом.

Блок «Инструкция по работе в сети» включает в себя требования и рекомендации по использованию программного обеспечения и поведения в локальной сети предприятия (рисунок 24).

Инструкция состоит из 5 пунктов:

- область применения;
- определения;
- общие положения;
- правила работы с компьютерами;
- порядок работы в корпоративной сети.

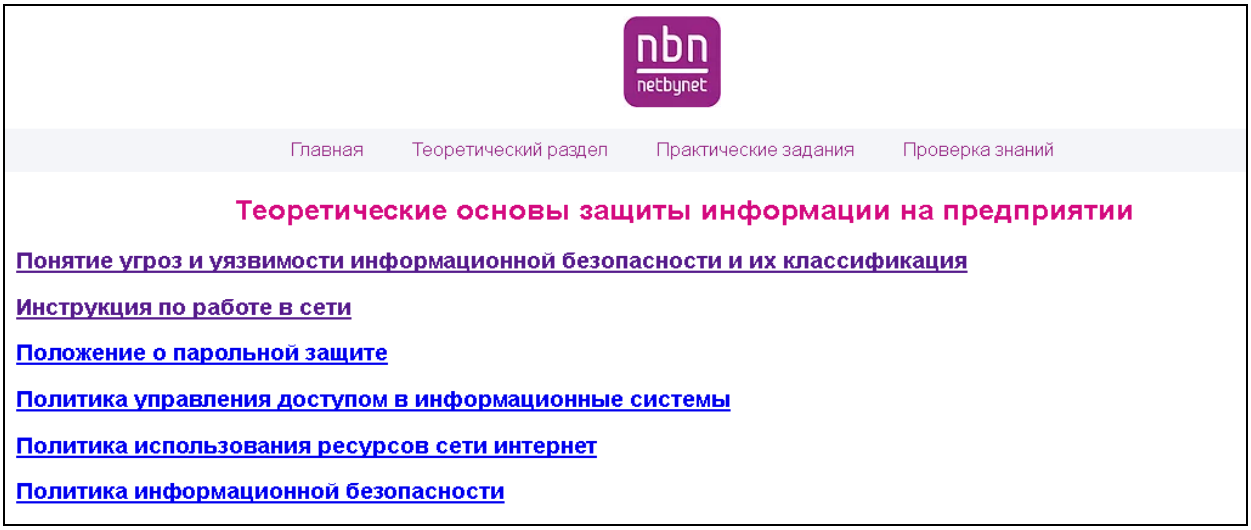
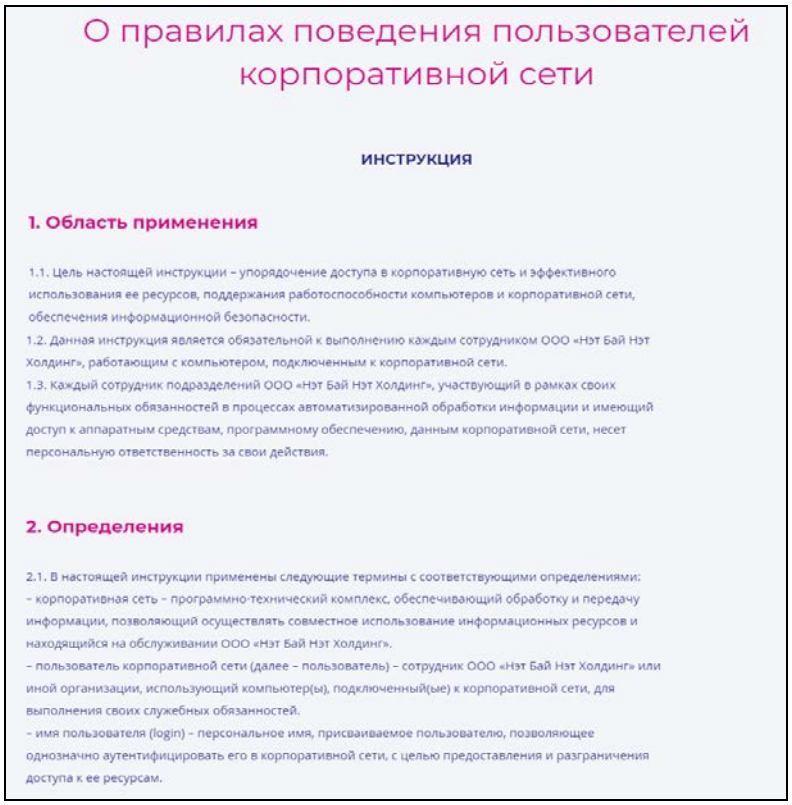


Рисунок 23 — Страница «Теоретический раздел»

Наиболее подробно расписан пятый пункт, так как именно он позволяет устранить наиболее частые угрозы в виде ошибок, допускаемых пользователями локальной сети. Данный порядок работы в сети содержит 4 пункта:

- общие правила подключения;
- порядок регистрации и работы пользователей;
- порядок работы пользователей с электронной почтой;
- порядок работы с ресурсами сети интернет.



О правилах поведения пользователей корпоративной сети

ИНСТРУКЦИЯ

1. Область применения

1.1. Цель настоящей инструкции – упорядочение доступа в корпоративную сеть и эффективного использования ее ресурсов, поддержания работоспособности компьютеров и корпоративной сети, обеспечения информационной безопасности.
1.2. Данная инструкция является обязательной к выполнению каждым сотрудником ООО «Нэт Бай Нэт Холдинг», работающим с компьютером, подключенным к корпоративной сети.
1.3. Каждый сотрудник подразделений ООО «Нэт Бай Нэт Холдинг», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным корпоративной сети, несет персональную ответственность за свои действия.

2. Определения

2.1. В настоящей инструкции применены следующие термины с соответствующими определениями:
– корпоративная сеть – программно-технический комплекс, обеспечивающий обработку и передачу информации, позволяющий осуществлять совместное использование информационных ресурсов и находящийся на обслуживании ООО «Нэт Бай Нэт Холдинг».
– пользователь корпоративной сети (далее – пользователь) – сотрудник ООО «Нэт Бай Нэт Холдинг» или иной организации, использующий компьютер(ы), подключенный(ые) к корпоративной сети, для выполнения своих служебных обязанностей.
– имя пользователя (login) – персональное имя, присваиваемое пользователю, позволяющее однозначно аутентифицировать его в корпоративной сети, с целью предоставления и разграничения доступа к ее ресурсам.

Рисунок 24 — Раздел «Инструкция по работе в сети»

Раздел «Запрещенное ПО» содержит список программного обеспечения, запрещенного к использованию на компьютерах, входящих в корпоративную сеть (рисунок 25):

- программы общения в сети, кроме ICQ или корпоративного аналога, устанавливаемого отделом по информационной безопасности (ОЗИ);
- программы прослушивания сетевого трафика (снифферы);
- сканеры безопасности (сканеры уязвимостей);
- сканеры портов;

- сканеры сетевых ресурсов;
- программы взлома/подбора паролей;
- иное программное обеспечение, при помощи которого можно нарушить работу компьютеров или других сетевых устройств, либо позволяющего получить доступ к закрытым сетевым ресурсам и сетевому оборудованию;
- игры и другие программы развлекательного характера;
- любое другое программное обеспечение (на усмотрение сотрудника ОЗИ).

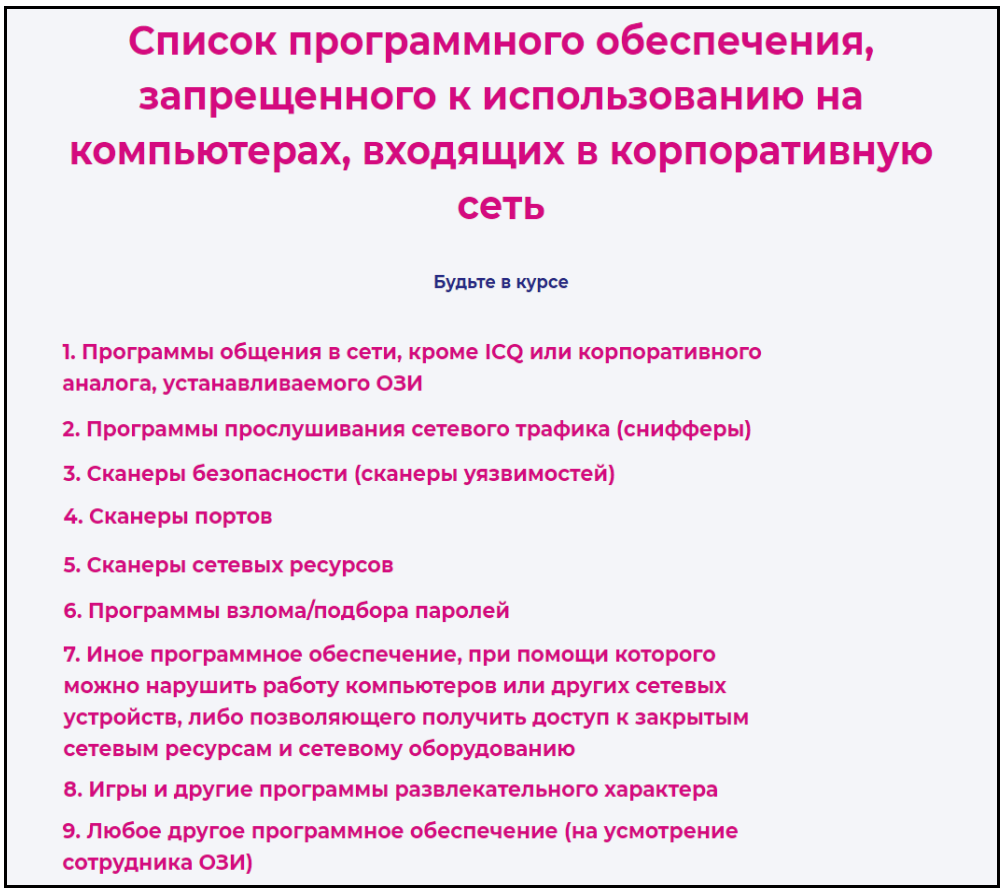


Рисунок 25 — Содержание раздела

Раздел «Практические задания» содержит гиперссылки на обещающие документы (рисунок 26).

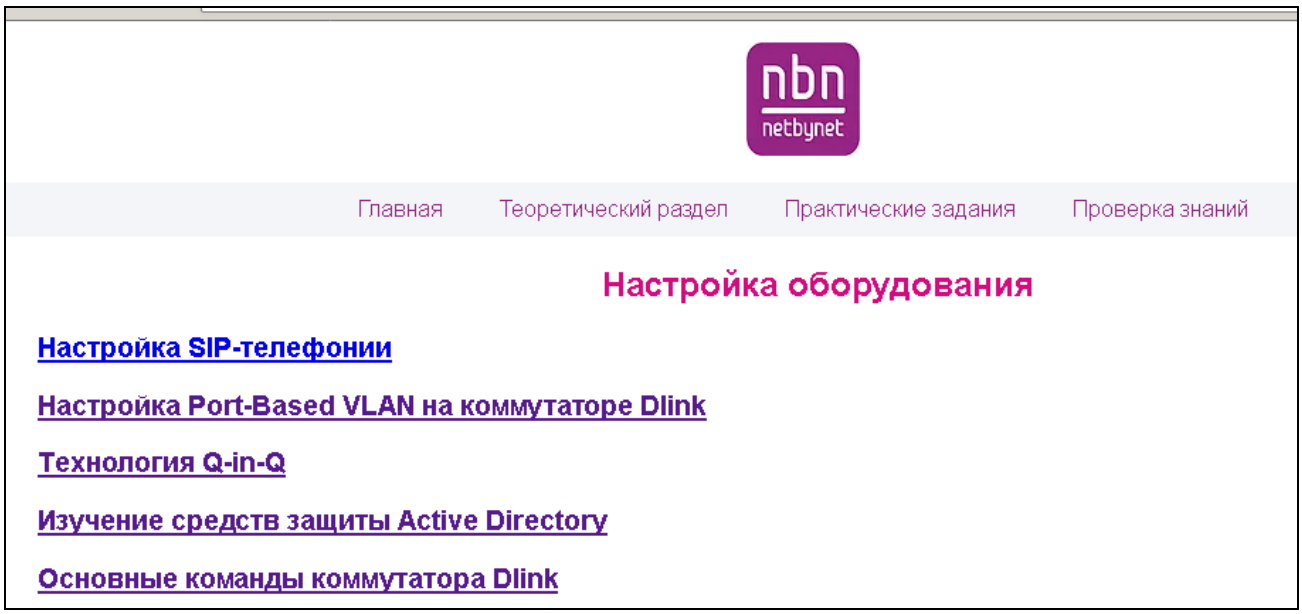


Рисунок 26 — Содержание раздела «Практические задания»

При нажатии на текст «Настройка SIP-телефонии» происходит перенаправление на страницу и подробной инструкцией как настроить SIP-телефон (рисунок 27).

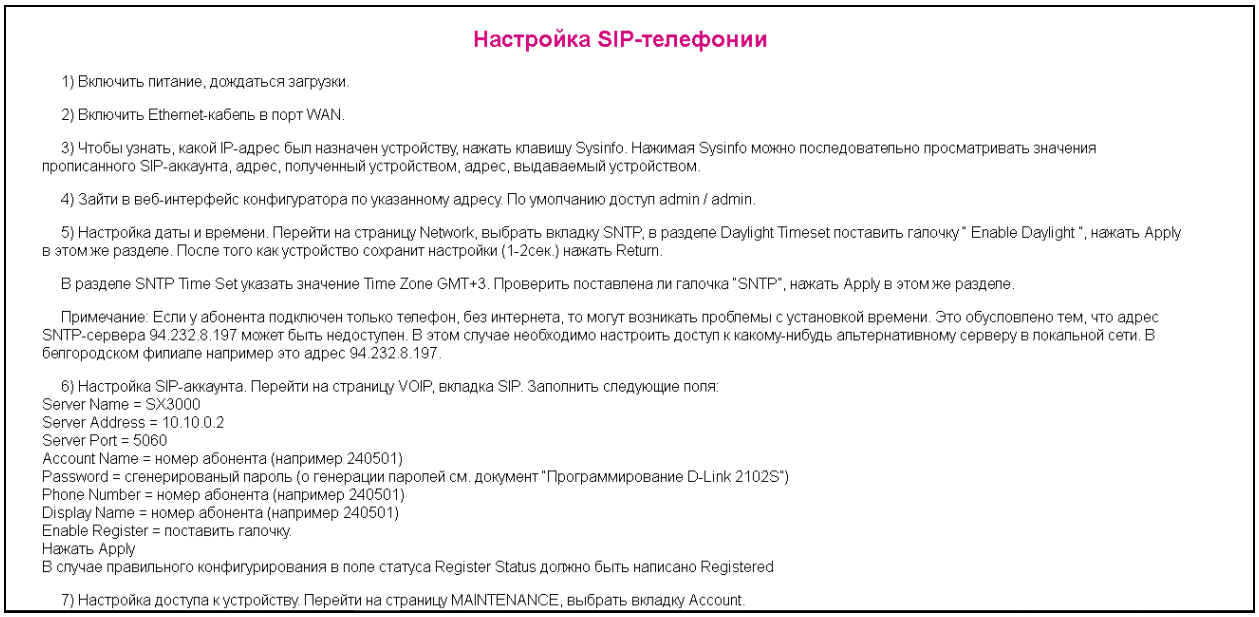


Рисунок 27 — Страница «Настройка SIP-телефонии»

Аналогично открываются остальные инструкции в данном разделе. Например, страница «Технология Q-in-Q» (рисунок 28).

Рисунок 28 — Страница «Технология Q-in-Q»

В результате тестирования приходим к выводу, что данный продукт работает и может использоваться в исследуемом предприятии.

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы были разработаны инструкции по безопасности локальной сети предприятия состоящее из нескольких блоков.

В ходе проектирования данной выпускной квалификационной работы проведено исследование теоретических вопросов в области информационной безопасности, а также выявление основных проблем, связанных с безопасностью современной корпоративной сети.

Обзор источников информации показал, что современной литературы по данной теме много. Большинство источников, которые удалось найти размещены в интернете в виде сайтов. Материал воспринимается не сложно в силу наглядного представления его на практике. Подобные готовые электронные продукты удалось найти в интернете, но их содержание не подходит для исследуемого предприятия, так как каждая организация имеет свою специфику защиты информации.

На конкретном примере проведен анализ деятельности ООО «Нэт Бай Нэт Холдинг», рассмотрено техническое и программное оснащение данной компании.

В качестве одной из мер по устранению недостатков в безопасности был разработан блок инструкций, который будет доступен всем пользователям ООО «Нэт Бай Нэт Холдинг», тем самым все пользователи будут оповещены о существующей на предприятии системы безопасности. В данных инструкциях были отображены основные действия сотрудников компании в случае угрозы, а также их обязанности по защиты информации, для того чтобы эта угроза не наступила.

Тестирование инструкций по безопасности локальной сети показало возможность его использования на предприятии.

В результате проделанной работы были решены следующие задачи:

- проанализированы литературные и интернет-источники по теме исследования.
- проанализирована компания на предмет уязвимостей в системе безопасности.
- реализованы электронные инструкции.

Таким образом, поставленные задачи можно считать полностью выполненными, а цель достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Варлатая С. К. Программно-аппаратная защита информации [Текст]: учебное пособие / С. К. Варлатая, М. В. Шаханова. — Владивосток: ДВГТУ, 2015. — 122 с.

2. Васильев В. В Информационная безопасность банка: внедряем СУ-ИБ [Текст] / В. В. Васильев // PC Week. — Москва: СК Пресс, 2014. — № 9-10. — С. 51—52.

3. Вихорев С. К. Как определить источники угроз [Текст] / С. К. Вихорев, Р. В. Кобцев // Открытые системы. — 2015. — № 7. — С. 8.

4. Гайдамакин Н. А. Информационная безопасность АИС, баз и банков данных [Текст] / Н. А. Гайдамакин. — Екатеринбург: ИОНЦ, 2016. — 42 с.

5. ГОСТ 7.1-2003. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления [Электронный ресурс]. — Введ. 30.06.2004. — Режим доступа: http://internet-law.ru/gosts/gost/1560/ (дата обращения: 22.03.2019).

6. ГОСТ 7.32-2001 СИБИД. Отчет о научно-исследовательской работе. Структура и правила оформления [Электронный ресурс]. — Введ. 01.07.2002. — Режим доступа: http://docs.cntd.ru/document/gost-7-32-2001-sibid (дата обращения: 22.03.2019).

7. ГОСТ 7.82-2001 СИБИД. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления [Электронный ресурс]. — Введ. 01.07.2002. — Режим доступа: http://docs.cntd.ru/document/1200025968 (дата обращения: 22.03.2019).

8. ГОСТ Р 7.0.12-2011 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила [Элек-

тронный ресурс]. — Введ. 01.09.2012. — Режим доступа: http://docs.cntd.ru/document/1200093114 (дата обращения: 22.03.2019).

9. Загинайлов Ю. Н. Комплексная система защиты информации на предприятии [Текст]: учебно-методическое пособие / Ю. Н. Загинайлов. — Барнаул: АлтГТУ, 2017. — 287 с.

10. Защита от внутренних и внешних угроз информационной безопасности с помощью InfoWatch Traffic Monitor и Cisco IronPort S-Series [Электронный ресурс]. — Режим доступа: https://www.infowatch.ru/ (дата обращения: 21.12.2018).

11. Змеев А. А. Анализ программных средств системы защиты информации от несанкционированного доступа в интегрированных системах безопасности [Текст] / А. А. Змеев // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций. — 2016. — № 1 — С. 2.

12. Использование электронных учебных пособий в учреждениях профессионального образования [Электронный ресурс]. — Режим доступа: https://moluch.ru/conf/ped/archive/72/4050/ (дата обращения: 22.03.2019).

13. Кораблев С. К. Внутренние угрозы: темная сторона информационной безопасности [Текст] / С. К. Кораблев // IT-Expert. — 2014. — №9. — С. 10.

14. КУБ — новый подход к управлению информационной безопасностью банка [Текст] // Information Security. — Москва: Groteck, 2015. — №5 — С. 7.

15. Лихотинский С. Н. Система управления информационной безопасностью в банках — время собирать камни [Текст] / С. Н. Лихотинский // Банкир. — 2015. — №10 — С. 17.

16. Лукоев О. С. Внутренние ИТ-угрозы не слабее внешних [Текст] / О. С. Лукоев // PC Week. — Москва: СК Пресс, 2015. — №44 — С. 50.

17. Магомедова Н. А. Средства защиты информации от несанкционированного доступа [Текст] / Н. А. Магомедова, М. К. Аливагабов // Вопросы структуризации экономики. — 2014. — №1 — С. 43.

18. Маркова Т. И. Классификация инсайдеров [Текст] / Т. И. Маркова, К. В. Захарова // Вестник Волжского университета им. В. Н. Татищева. — 2015. — №15 — С. 23.

19. Мельников В. П. Информационная безопасность и защита информации [Текст]: учебное пособие / В. П. Мельников. — Москва: Академия, 2015. — 256 с.

20. Норткат С. П. Информационная безопасность и защита информации [Текст] / С. П. Норткат, Д. Новак. — Москва: Вильямс, 2015. —312 с.

21. О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 224-ФЗ (ред. от 31.12.2017). — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 18.11.2018).

22. О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком [Электронный ресурс]: Федеральный закон от 27.07.2010 № 224-ФЗ (ред. от 27.12.2018). — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_103037/ (дата обращения: 14.11.2018).

23. О техническом регулировании [Электронный ресурс]: Федеральный закон от 27.12.2002 № 184-ФЗ (ред. от 29.07.2017). — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/ (дата обращения: 18.11.2018).

24. Общие вопросы технической защиты информации [Электронный ресурс]. — Режим доступа: http://www.intuit.ru/studies/courses/2291/591/info (дата обращения: 14.01.2019).

25. Олифер В. Г. Безопасность компьютерных сетей [Текст] / В. Г. Олифер, Н. А. Олифер. — Москва: Телеком, 2017. — 644 с.

26. Официальный сайт Zecurion [Электронный ресурс]. — Режим доступа: http://www.zecurion.ru/products/ (дата обращения: 11.01.2019)

27. Официальный сайт компании ООО «Нэт Бай Нэт Холдинг» Электронный ресурс]. — Режим доступа: http://www.netbynet.ru/ (дата обращения: 11.01.2019).

28. Официальный сайт НПФ «Кристалл» [Электронный ресурс]. — Режим доступа: http://www.npf-crystall.ru/products.htm (дата обращения: 21.01.2019).

29. Плетнев П. В. Методика оценки рисков информационной безопасности [Текст] / П. В. Плетнев, В. М. Белов // Доклады ТУСУРа. — 2014. — № 1. — С. 25.

30. Пять проблем и тенденций информационной безопасности: чего ожидать в 2018 году [Электронный ресурс]. — Режим доступа: https://habr.com/company/globalsign/blog/348690 (дата обращения: 06.11.2018).

31. Смирнов Д. К. Борьба с утечками данных [Текст] / Д. К. Смирнов// LETA IT-company. — 2016. — № 23. — С. 19.

32. Стандарт Предприятия России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» [Электронный ресурс]: Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 «СТО БР ИББС-1.2-2014» (принят и введен в действие Распоряжением Предприятия России от 17.05.2014 № Р-399). — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_163807/ (дата обращения: 18.12.2018).

33. Титова Е. И. О создании электронного учебника [Текст] / Е. И. Титова, А. В. Чапрасова // Молодой ученый. — 2015. — №3. — С. 855.

34. Угрозы информационной безопасности: обзор и оценка [Электронный ресурс]. — Режим доступа: http://rus.safensoft.com/security.phtml?c=791 (дата обращения: 18.01.2019).

35. Утебов Д. Р. Классификация угроз в системах управления базами данных [Текст] / Д. Р.Утебов, С. В. Белов // Вестник АГТУ. — 2016. — № 1. — С. 42.

36. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях [Текст] / В. Ф. Шаньгин. — Москва: ДМК Пресс, 2015. — 416 с.

37. Шаньгин В. Ф. Информационная безопасность и защита информации [Текст] / В. Ф. Шаньгин. — Москва: ДМК Пресс, 2017. — 702 с.

38. Шарафутдинов А. Г. Виды угроз безопасности в экономических информационных системах [Текст] / А. Г. Шарафутдинов // Экономика и социум. — 2016. — № 1. — С. 20.

39. Шейдаков Н. Е. Физические основы защиты информации [Текст] / Н. Е. Шейдаков, О. В. Серпенинов, Е. Н Тищенко. — Москва: РИОР, Инфра-М, 2017. — 208 с.

40. Шипилов В. В. Обеспечение информационной безопасности в банках: итоги анкетирования [Текст] / В. В. Шипилов // V Юбилейный Уральский форум «Информационная безопасность банков». — Екатеринбург, 2015. — 25 с.

ПРИЛОЖЕНИЕ

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования

Кафедра информационных систем и технологий

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль «Информатика и вычислительная техника»

Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой ИС

_____ И.А. Суслова
подпись и.о. фамилия

« ___ » _____ 2019 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента (ки) ***5*** курса группы *ЗИБ-501*

Колотова Ильи Евгеньевича
фамилия, имя, отчество полностью

1. Тема ***Электронные инструкции по обеспечению безопасности локальной сети предприятия***

утверждена распоряжением по институту от «_____» _____
_____ 20 г. № ___

2. Руководитель ***Шайдуров Андрей Александрович***
фамилия, имя, отчество полностью

доцент (ученая степень) *к.пед.н.* (ученое звание) *доцент кафедры ИС* (должность) *РГППУ* (место работы)

3. Место преддипломной практики *ООО «Нэт Бай Нэт Холдинг»*

4. Исходные данные к ВКР
Шаньгин В. Ф. Информационная безопасность и защита информации [Текст] / В. Ф. Шаньгин. — Москва: ДМК Пресс, 2017. — 702 с.

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
выявить основные системы и методы защиты от внутренних и внешних угроз;
разработать и внедрить электронные инструкции по защите локальной сети предприятия

ООО «Нэт Бай Нэт Холдинг».

6. Перечень демонстрационных материалов *презентация выполненная в MS Power Point, электронные инструкции для сотрудников предприятия.*

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе	12.12.2018	10%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		60%	подпись
2.1	Анализ предприятия.	22.12.2018	10%	подпись
2.2	Анализ состояния информационной безопасности предприятия.	24.12.2018	10%	подпись
2.3	Разработка обоснования разработки и внедрения средств защиты информации на предприятии	26.12.2018	10%	подпись
2.4	Разработка электронных инструкций	28.12.2018	15%	подпись
2.5	Исправление недочетов	30.12.2018	15%	подпись
3	Оформление текстовой части ВКР	03.01.2019	10%	подпись
4	Выполнение демонстрационных материалов к ВКР	07.01.2019	10%	подпись
5	Нормоконтроль	15.02.2019	5%	подпись
6	Подготовка доклада к защите в ГЭК	18.02.2019	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ _____ *Задание получил* _____

_____ _____

подпись дата

подпись студента дата

9. Дипломная работа и все материалы проанализированы.

Считаю возможным допустить ***Колотова И.Е.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____

подпись дата

10. Допустить ***Колотова И.Е.*** к защите выпускной квалификационной работы

фамилия и. о. студента

в государственной экзаменационной комиссии (протокол заседания кафедры от «_____» _____ 20_____г., № _____ _____)

И.о. заведующего кафедрой _____ _____

подпись дата